EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	52	"password dictionary"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/27 13:52
S2	46239	(password credential) and check$3	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/27 13:53
S3	4504	S2 and strength	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/27 13:54
S4	407	S3 and proactive	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/27 13:54
S5	37	S4 and ("713"/$.ccls.)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/27 16:32
S6	4	("5394471" "5588056").did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/27 15:38
S7	1	"5394471".PN.	USPAT; USOCR	OR	ON	2006/11/27 15:39
S8	21	("4440976" | "4926475" | "4974191" | "5199069" | "5307409").PN. OR ("5394471"). URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2006/11/27 15:40

EAST Search History

S9	155	("3581072" | "3956615" | "4754428" | "4799156" | "4805099" | "4805134" | "4882474" | "4962475" | "4989141" | "4992940" | "5032989" | "5063507" | "5107443" | "5136501" | "5164897" | "5168446" | "5189608" | "5197004" | "5197005" | "5204947" | "5235680" | "5243515" | "5251294" | "5257366" | "5261102" | "5262943" | "5263157" | "5263158" | "5283731" | "5297249" | "5299123" | "5301105" | "5309437" | "5319542" | "5325297" | "5335346" | "5339361" | "5339392" | "5347632" | "5355474" | "5367619" | "5367621" | "5386525" | "5394471" | "5406475" | "5408655" | "5410693" | "5412774" | "5414809" | "5416694" | "5418942" | "5426780" | "5428606" | "5428778" | "5448724" | "5455945" | "5459863" | "5471617" | "5483586" | "5495412" | "5502637" | "5506984" | "5513126" | "5530852" | "5537546" | "5537590" | "5542024" | "5544255" | "5544360" | "5553239" | "5557518" | "5559958" | "5564119" | "5572643" | "5592375" | "5608903" | "5623601" | "5623652" | "5625781" | "5630125" | "5633910" | "5638457" | "5649192" | "5655077" | "5659741" | "5659742" | "5664115" | "5664207" | "5675507" | "5677953" | "5678041" | "5682525" | "5684951" | "5694546" | "5699526" | "5706507" | "5708780" | "5710887" | "5710918" | "5715314" | "5715402" | "5717923" | "5721827" | "5721906" | "5721908" | "5724424" | "5727156" | "5729682" | "5732219" | "5734718" | "5734823" | "5737395" | "5737592" | "5742769" | "5742845" | "5745556" | "5748188" | "5748740" | "5748783" | "5754939" | "5754981" | "5757917" | "5758324" | "5761649" | "5761656").PN. OR ("5761661" | "5761662" | "5761673" | "5778367" | "5784608" | "5790793" | "5802299" | "5802497" | "5812776" | "5813006" | "5819285" | "5822745" | "5826241" | "5832497" | "5835712" | "5835896" | "5838903" | "5842173" | "5850446" | "5862323" | "5870552" |	US-PGPUB; USPAT; USOCR	OR	ON	2006/11/27 15:49

EAST Search History

S10	12597	(password keyword credential) near5 (generat$3 creat$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/27 16:33
S11	1924	S10 and ("713"/$.ccls. 382/115.ccls "340"/$.ccls.)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 10:52
S12	1335	S11 and (@ad<="20021011" or @rlad<="20021011")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 10:36
S13	15370	((proactive check$3 select$3) with password)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 10:38
S14	14	((proactive check$3 select$3) with password) near5 strength	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 10:38
S15	12610	(password keyword credential) near5 (generat$3 creat$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 10:52
S16	2700	S15 and ("713"/$.ccls. 382/115.ccls "340"/$.ccls. "726"/$.ccls.)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 10:53
S17	1822	S16 and (@ad<="20021011" or @rlad<="20021011")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 10:53
S18	2464	S15 and ("713"/$.ccls. "726"/$.ccls.)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 16:27
S19	124692	"l2" and (@ad<="20021011" or @rlad<="20021011")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 10:54
S20	1653	S18 and (@ad<="20021011" or @rlad<="20021011")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 10:54
S21	10967	(password keyword) with (history reoccur$5 list$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 14:58

EAST Search History

S22	65	(password keyword) with (reoccur$5 list$3) near5 history	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 14:29
S23	41	S22 and (@ad<="20021011" or @rlad<="20021011")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 14:47
S24	355	((password keyword credential) with match) near5 (history list profile)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 14:48
S25	261	S24 and (@ad<="20021011" or @rlad<="20021011")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 14:48
S26	356	password near5 history	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 14:58
S27	219	S26 and (@ad<="20021011" or @rlad<="20021011")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 16:11
S28	44	"password history"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 16:13
S29	26	S28 and (@ad<="20021011" or @rlad<="20021011")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 16:24
S30	7519	((password passcode keyword credential) near5 log$3) and (not (readable))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 16:27
S31	5348	S30 and (@ad<="20021011" or @rlad<="20021011")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 16:27
S32	0	S15 and (726/3-10.ccls)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 16:28
S33	1197	S15 and (726/3-10.ccls or "726"/$.ccls.)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 16:29

EAST Search History

S34	256	S15 and (726/3-10.ccls or 713/183-184.ccls. 713/202.ccls.)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 17:10
S35	0	(password keyword passcode secret) near5 (patern and matching)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 17:11
S36	1505	(password keyword passcode secret) near5 pattern	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 17:12
S37	874	S36 and (match$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 17:13
S38	16	S37 and ((726/3-10.ccls or 713/183-184.ccls. 713/202.ccls.) and (@ad<="20021011" or @rlad<="20021011"))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/28 17:13
S39	3566	(password$2 passcode$2 keyword$2) near5 (validat$3 confirmat$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/29 08:25
S40	2641	S39 and (@ad<="20021011" or @rlad<="20021011")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/29 08:26
S41	79	S40 and (726/4-5.ccls.)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/29 08:53
S42	121	(logon near5 procedure) with (password$2 keyword$2 passcode$2)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/29 08:55
S43	9	S42 and ((@ad<="20021011" or @rlad<="20021011") and (726/4-5. ccls.))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/29 08:54
S44	161	(registrat$3 near5 procedure) with (password$2 keyword$2 passcode$2)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/29 08:56
S45	2	S44 and ((@ad<="20021011" or @rlad<="20021011") and (726/4-5. ccls.))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/29 10:03

EAST Search History

S46	126	S44 and (@ad<="20021011" or @rlad<="20021011")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/29 10:04
S47	46436	(password credential) and check$3	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/30 11:24
S48	4521	S47 and strength	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/30 11:24
S49	409	S48 and proactive	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/30 12:37
S52	5041	(character$2 near5 string$2) near5 (locat$3 position$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/30 16:40
S53	8003	(character$2 near5 string$2) near5 (examin$5 extract$3 locat$3 position$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/30 17:46
S54	2660	(password$2 passphrase$2 keyword$2 credential$2) near5 (strength rank$3 measur$6 examin$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/30 17:02
S55	68	S53 and S54	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/30 17:03
S56	5008	(character$2 near5 string$2) near5 (position$2 locat$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/30 17:32
S57	36	S54 and S56	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/30 17:32
S58	10680	(character$2 near5 string$2) with (examin$5 extract$3 locat$3 position$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/30 17:46
S59	108	S54 and S58	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/11/30 17:46

EAST Search History

S60	2	"7120302".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/12/06 14:46
S61	102955	(rank$3 level$2 near5 (password passcode passphrase))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/12/06 15:47
S62	2904	(rank$3 level$2) near5 (password passcode passphrase)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/12/06 15:47
S63	84	S62 and (713/183-184.ccls. 726/25.ccls. 726/3.ccls.)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/12/06 16:14
S64	8775	(password passphrase "pass phrase") near5 (creat$3 generat$3 produc$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/12/06 16:39
S65	348	S64 and (713/183-184.ccls. 726/25.ccls. 726/3.ccls.)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/12/06 17:39
S66	255	S65 and (@ad<="20021011" or @rlad<="20021011")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/12/06 16:33
S67	37	S62 and S65 and S66	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/12/06 16:34
S68	418	(password passphrase "pass phrase") near5 (strong weak)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/12/06 16:40
S69	266	S68 and (@ad<="20021011" or @rlad<="20021011")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/12/06 17:03
S70	3350	(authent$7 near5 (rank$3 level$2)) and (@ad<="20021011" or @rlad<="20021011")	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/12/06 17:06
S71	1433	713/183-184.ccls. 726/25.ccls. 726/3.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/12/06 17:04

EAST Search History

S72	73	S70 and S71	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/12/07 15:29
S73	3	"20020144128"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/12/06 17:49
S74	2	"7058817".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/12/07 13:12
S75	45	"password history"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2006/12/07 18:04

STIC search for 10677277

Inventor - Patents

Set	Items	Description
S1	34	S AU=(SANAI, D? OR SANAI D?)
S2	0	S AU=(DAIJI, S? OR DAIJI S?)
S3	404	S AU=(ARIMOTO, M? OR ARIMOTO M?)
S4	167	SELECT AU= "ARIMOTO M"
S5	5	SELECT AU= "ARIMOTO MICHIHARU"
S6	3	SELECT AU= "ARIMOTO, M" OR AU= "ARIMOTO, MICHIHARU"
S7	2	S AU=(MICHIHARU, A? OR MICHIHARU A?)
S8	2035	S AU=(MISHIMA, T? OR MISHIMA T?)
S9	805	SELECT AU= "MISHIMA T"
S10	140	SELECT AU= "MISHIMA TAKASHI"
S11	15	SELECT AU= "MISHIMA, T" OR AU= "MISHIMA, TAKASHI"
S12	209	S AU=(TAKASHI, M? OR TAKASHI M?)
S13	95	SELECT AU= "TAKASHI M"
S14	0	SELECT AU= "TAKASHI, M"
S15	4122	S AU=(SEKI, H? OR SEKI H?)
S16	1704	SELECT AU= "SEKI H"
S17	7	SELECT AU= "SEKI HIDENOBU" OR AU= "SEKI HIDENOBU SECURITY FRIDAY CO LTD"
S18	3	SELECT AU= "SEKI, H" OR AU= "SEKI, HIDENOBU"
S19	0	S AU=(HIDENOBU, S? OR HIDENOBU S?)
S20	6780	S S1:S18
S21	137	S S20 AND IC=H04L
S22	780115	S PASSWORD? ? OR PASSCODE? ? OR PASSPHRASE? ? OR PASS()(WORD? ? OR CODE? ? OR PHRASE? ?) OR PIN OR PINS OR CREDENTIAL? ?
S23	127	S S20 AND S22
S24	5927	S S22 (5N) (STRENGTH OR STRONG?? OR GOOD OR HIGH()QUALITY OR "NOT" (3W) (GUESS?? OR DEDUCE? ? OR (WORK OR FIGURE OR FIND)()OUT OR DISCOVER?? OR DETERMINE? ? OR STOLEN OR STEAL OR EXTORT??) OR VULNERABL? ?)
S25	4	S S20 AND S24
S26	4	IDPAT (sorted in duplicate/non-duplicate order)

S27 2 IDPAT (primary/non-duplicate records only)

S28 2 S S23 AND IC=H04L

S29 1 S S28 NOT S27

S30 17 S S23 AND IC=G06F

S31 15 S S30 NOT (S27 OR S29)

S32 15 IDPAT (sorted in duplicate/non-duplicate order)

S33 11 IDPAT (primary/non-duplicate records only)

; show files

[File 347] **JAPIO** Dec 1976-2006/Jul(Updated 061116)
(c) 2006 JPO & JAPIO. All rights reserved.

[File 348] **EUROPEAN PATENTS** 1978-2006/ 200646
(c) 2006 European Patent Office. All rights reserved.
**File 348: For important information about IPCR/8 and forthcoming changes to the IC= index, see HELP NEWSIPCR.*

[File 349] **PCT FULLTEXT** 1979-2006/UB=20061123UT=20061116
(c) 2006 WIPO/Thomson. All rights reserved.
**File 349: For important information about IPCR/8 and forthcoming changes to the IC= index, see HELP NEWSIPCR.*

[File 350] **Derwent WPIX** 1963-2006/UD=200675
(c) 2006 The Thomson Corporation. All rights reserved.
**File 350: DWPI has been enhanced to extend content and functionality of the database. For more info, visit http://www.dialog.com/dwpi/.*

Your application

27/5/1 (Item 1 from file: 350)
Derwent WPIX
(c) 2006 The Thomson Corporation. All rights reserved.

0014143953 *Drawing available*
WPI Acc no: 2004-328733/
XRPX Acc No: N2004-262269
Password strength checking method involves generating next password candidate when input password does not match with generated plaintext password candidate, and calculating number of candidates when match is determined
Patent Assignee: YAMATAKE CORP (YAMA-N); YAMATAKE HONEYWELL CO LTD (HONF)
Inventor: **ARIMOTO M**; ARIMOTO N; **MISHIMA T; SANAI D** ; SEKI E; **SEKI H**

Patent Family (4 patents, 2 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
US 20040073815	A1	20040415	US 2003677277	A	20031003	200430	B
JP 2004133720	A	20040430	JP 2002298190	A	20021011	200430	E
JP 2004199320	A	20040715	JP 2002366243	A	20021218	200446	E
JP 2004199322	A	20040715	JP 2002366258	A	20021218	200446	E

Priority Applications (no., kind, date): JP 2002366258 A 20021218; JP 2002298190 A 20021011; JP 2002366243 A 20021218

Patent Details

Patent Number	**Kind**	**Lan**	**Pgs**	**Draw**	**Filing Notes**	
US 20040073815	A1	EN	47	31		
JP 2004133720	A	JA	13			
JP 2004199320	A	JA	16			
JP 2004199322	A	JA	11			

Alerting Abstract US A1
NOVELTY - A plaintext password candidate is generated according to generation procedure same as the procedure used by a password guessing tool. The next password candidate is generated when the input password does not match with the generated **password** candidate. The **strength** of the input **password** is determined based on the number of the generated password candidates when the match is determined.
DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

1. a **password strength** checking apparatus;
2. a program for checking **password strength**;
3. a recorded medium storing **password strength** checking program;
4. a **password** creation assisting method;
5. a program for assisting password creation;
6. password creation method; and
7. a password creating program.

USE - For **checking** strength **of** password for access approval of computer system used in office.
ADVANTAGE - **The password** strength can be calculated in practical duration of time, thereby enabling accurate checking of **the password** strength and enhancing security for internal information.
DESCRIPTION OF DRAWINGS - The figure shows the block diagram of **the password** strength checking apparatus.

Title Terms /Index Terms/Additional Words: PASSWORD; STRENGTH; CHECK; METHOD; GENERATE; CANDIDATE; INPUT; MATCH; CALCULATE; NUMBER; DETERMINE

Class Codes

International Patent Classification

IPC	**Class Level**	**Scope**	**Position**	**Status**	**Version Date**
G06F-015/00; H04L-009/00			Main		"Version 7"
H04L-009/32			Secondary		"Version 7"

US Classification, Issued: 713202000

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-N02B1B; T01-S03

Your Japanese application?

29/5/1 (Item 1 from file: 347)
JAPIO
(c) 2006 JPO & JAPIO. All rights reserved.
08020961 **Image available**

PASSWORD STRENGTH CHECKING METHOD AND DEVICE, PASSWORD STRENGTH CHECKING PROGRAM, AND RECORDING MEDIUM RECORDED WITH THE PROGRAM

Pub. No.: 2004-133720 [JP 2004133720 A]
Published: April 30, 2004 (20040430)
Inventor: MISHIMA TAKASHI
SEKI EISHIN
ARIMOTO NORIJI
SANAI DAIJI
Applicant: YAMATAKE CORP
Application No.: 2002-298190 [JP 2002298190]
Filed: October 11, 2002 (20021011)
International Class: G06F-015/00; **H04L-009/32**

ABSTRACT

PROBLEM TO BE SOLVED: To provide a new **password** strength checking technique that can objectively and accurately check the strength of a **password**.

SOLUTION: When a **password** to be checked is input, a plaintext **password** candidate is generated according to the same generation procedure that is used in a **password** cracking tool, and the generated **password** candidate is checked for matching against the input **password**. Upon a mismatching result, an instruction is made to generate the next **password** candidate, so that **password** candidates are sequentially generated until the generated **password** candidate matches the input **password**. Upon a matching result, the strength of the input **password** is decided in dependence on the number of **password** candidates generated, and information on the decided **password** strength is output. A numerically expressed **password** strength can be computed in practical time.

COPYRIGHT: (C)2004,JPO

Wrong date

33/5/1 (Item 1 from file: 350)
Derwent WPIX
(c) 2006 The Thomson Corporation. All rights reserved.

0014381209 *Drawing available*
WPI Acc no: 2004-570258/
XRPX Acc No: N2004-451024

Password input table creating method, involves creating password input table by randomly entering possible characters to be used for password, in entry fields of table which have no inputted characters

Patent Assignee: YAMATAKE CORP (YAMA-N); YAMATAKE HONEYWELL CO LTD (HONF)
Inventor: **ARIMOTO M**; ARIMOTO N; **SANAI D**

Patent Family (2 patents, 2 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
US 20040139331	A1	20040715	US 2004750844	A	20040105	200455	B
JP 2004265359	A	20040924	JP 200386864	A	20030327	200463	E

Priority Applications (no., kind, date): JP 20032849 A 20030109; JP 200386864 A 20030327

Patent Details

Patent Number	**Kind**	**Lan**	**Pgs**	**Draw**	**Filing Notes**
US 20040139331	A1	EN	34	24	
JP 2004265359	A	JA	22		

Alerting Abstract US A1
NOVELTY - The method involves displaying a creation table having multiple entry fields, on a display, where each field is an input area for one character. Each character, composing a **password** to be inputted into a computer, is entered through an interactive process. A **password** input table is created by randomly entering possible characters to be used for a **password**, in entry fields of table which have no inputted characters.
DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

a. a **password** input table creating apparatus

b. a **password** input table creating program used to implement a **password** input table creating method.

USE - Used for creating a **password** input table that is referred when inputting a **password** into a computer (claimed).
ADVANTAGE - The **password** input table shows the **password** in a form that is readable only by the user inputting the **password** and thereby provides a robust **password** which is difficult for a user to remember. The method thus avoids the necessity for writing the **password** on the paper to enter it in the computer, and provides security.
DESCRIPTION OF DRAWINGS - DESCRIPTION OF DRAWING - The drawing shows a **password** input table creating apparatus.
1 **Password** input table creating apparatus
10 Input/output device
11 Routine
12 **Password** creating program
13 Word dictionary
14 **Password** input table creating program

Title Terms /Index Terms/Additional Words: **PASSWORD**; INPUT; TABLE; METHOD; RANDOM; ENTER; POSSIBILITY; CHARACTER; FIELD; NO

Class Codes

International Patent Classification

IPC	**Class Level**	**Scope**	**Position**	**Status**	**Version Date**
G06F-015/00; H04K-001/00			Main		"Version 7"

US Classification, Issued: 713184000

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-J12C; T01-N02B1B; T01-S03

33/5/4 (Item 4 from file: 350)
Derwent WPIX
(c) 2006 The Thomson Corporation. All rights reserved.

0013499520 *Drawing available*
WPI Acc no: 2003-592046/
XRPX Acc No: N2003-471479
Security countermeasure execution apparatus overwrites random password registered into computer, when user trial to log-on to computer by designating user identification and random password is success
Patent Assignee: YAMATAKE HONEYWELL CO LTD (HONF)
Inventor: ARIMOTO N; HORI M; **MISHIMA T**; **SANAI D**; SEKI E

Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
JP 2003203051	A	20030718	JP 2002550	A	20020107	200356	B

Priority Applications (no., kind, date): JP 2002550 A 20020107

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes
JP 2003203051	A	JA	16	18	

Alerting Abstract JP A
NOVELTY - An acquisition unit acquires the user identifier information registered into a computer (1). A random **password** is generated. A trial to log-on to computer is carried out by designating the user identifier information and the random **password**. The utilization of the computer by the user is disturbed by overwriting the random **password** registered after trail success.
DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

8. security countermeasure execution method;

9. security countermeasure execution program; and

10. recorded medium storing countermeasure execution program.

USE - Security countermeasure execution apparatus.
ADVANTAGE - The problem originating in the random **password** is prevented.
DESCRIPTION OF DRAWINGS - The figure shows the block diagram of security countermeasure execution apparatus. (Drawing includes non-English language text).
1 computer for security countermeasure
2-1-2-n management computer
3-1-3-m user terminal

Title Terms /Index Terms/Additional Words: SECURE; EXECUTE; APPARATUS; RANDOM; **PASSWORD**; REGISTER; COMPUTER; USER; TRIAL; LOG; DESIGNATED; IDENTIFY; SUCCESS

Class Codes

International Patent Classification

IPC	Class Level	Scope	Position	Status	Version Date
G06F-015/00			Main		"Version 7"

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-J; T01-S03

Good art - wrong date

33/5/6 (Item 6 from file: 347)
JAPIO
(c) 2006 JPO & JAPIO. All rights reserved.
08086563 **Image available**
PASSWORD PREPARATION METHOD AND PASSWORD PREPARATION PROGRAM

Pub. No.: 2004-199322 [JP 2004199322 A]
Published: July 15, 2004 (20040715)
Inventor: MISHIMA TAKASHI
SANAI DAIJI
Applicant: YAMATAKE CORP
Application No.: 2002-366258 [JP 2002366258]
Filed: December 18, 2002 (20021218)
International Class: G06F-015/00

ABSTRACT

PROBLEM TO BE SOLVED: To provide new **password** preparation technology to prepare a **password** whose intensity is ensured.

SOLUTION: Under the consideration that the intensity of a **password** is made to correspond to the generation order of **password** candidates generated by a **password** presuming tool used for brute force attack, a user is made to input the intensity of the **password**, the generation order corresponding to the inputted intensity of the **password** is acquired, and a **password** is prepared by the **password** presuming tool on the basis of the result. Thus, it is possible to prepare a **password** whose intensity, that is, whose resistance to the brute force attack is guaranteed in two years, for example. Therefore, it is possible for a user to use the **password** without any anxiety.

COPYRIGHT: (C)2004,JPO&NCIPI

Your Japanese priority application

33/5/7 (Item 7 from file: 347)
JAPIO
(c) 2006 JPO & JAPIO. All rights reserved.
08086561 **Image available**
PASSWORD PREPARATION SUPPORT METHOD AND PROGRAM

Pub. No.: 2004-199320 [JP 2004199320 A]
Published: July 15, 2004 (20040715)
Inventor: MISHIMA TAKASHI
SANAI DAIJI
Applicant: YAMATAKE CORP
Application No.: 2002-366243 [JP 2002366243]

Filed: December 18, 2002 (20021218)
International Class: G06F-015/00

ABSTRACT

PROBLEM TO BE SOLVED: To provide a new **password** preparation support technology for analyzing which part of a **password** is strong, and which part is weak, and for outputting it.

SOLUTION: The number of generation until a **password** candidate having a character string to be checked is generated at first is acquired by using a **password** candidate generating tool for generating the **password** candidate of a plaintext according to a generation procedure which is the same as that to be used by a **password** presuming tool, and the intensity of the character string to be checked is calculated according to this number of generation. Also, information showing which position of a table used for brute force attack is registered with each of the characters of the **password** is acquired, and the intensity of each of the characters of the **password** is calculated according to this information. Also, the character string whose length is lengthened by every character is extracted with the leading character of the **password** as a start character, and the number of generation until the **password** candidate having the character string is generated at first is acquired, and the transition value of the character intensity of the **password** is calculated according to this value.

COPYRIGHT: (C)2004,JPO&NCIPI

33/5/11 (Item 11 from file: 347)
JAPIO
(c) 2006 JPO & JAPIO. All rights reserved.
02126873 **Image available**
PASSWORD SYSTEM

Pub. No.: 62-043773 [JP 62043773 A]
Published: February 25, 1987 (19870225)
Inventor: KANO MITSUNARI
TAKASHI MORIHIKO
Applicant: HITACHI LTD [000510] (A Japanese Company or Corporation), JP (Japan)
Application No.: 60-183536 [JP 85183536]
Filed: August 21, 1985 (19850821)
International Class: [4] **G06F-015/30**; G06K-017/00; G07D-001/00; G07F-007/08
JAPIO Class: 45.4 (INFORMATION PROCESSING -- Computer Applications); 29.4 (PRECISION INSTRUMENTS -- Business Machines); 45.3 (INFORMATION PROCESSING -- Input Output Units)
JAPIO Keyword: R087 (PRECISION MACHINES -- Automatic Banking)
Journal: Section: P, Section No. 599, Vol. 11, No. 230, Pg. 101, July 28, 1987 (19870728)

ABSTRACT
PURPOSE: To detect easily the foul use of a card at the device side by preparing plural **password** including an emergency code in addition to a normal **password** for a user and selecting optionally the right use with each **password**.

CONSTITUTION: For instance, a **password** C1 is prepared for the normal use of a user together with other codes C2-C4 used for emergency respectively. A **password** supplied from the user through a keyboard 3 is sent to a control part 5. The part 5 carries out a transaction as desired by the user when the code C1 is supplied. If the input code is not coincident with any of those **passwords** C1-C4, the part 5 decides a keying mistake and allows the retry. While an emergency signal is produced on an emergency information signal line 8 consisting of a wire or wireless signal line, etc. and led to outside in case the input code is coincidence with either one of **passwords** C1-C4. At the same time, a normal transaction is permitted as desired by the user. In such a way, the probability is greatly reduced for the foul use of a card.

Inventor - NPL (note: no appropriate references found.)

```
Set   Items  Description
S1      13  S AU=(SANAI, D? OR SANAI D?)
S2     220  SELECT AU= "ARIMOTO M"
S3      60  SELECT AU= "ARIMOTO, M" OR AU= "ARIMOTO, M."
S4       0  S AU=(MICHIHARU, A? OR MICHIHARU A?)
S5       0  S AU=(DAIJI, S? OR DAIJI S?)
S6     647  SELECT AU= "MISHIMA T"
S7      49  SELECT AU= "MISHIMA TAKASHI"
S8     684  SELECT AU= "MISHIMA, T" OR AU= "MISHIMA, T."
S9      19  SELECT AU= "MISHIMA, TAKASHI"
S10    206  SELECT AU= "TAKASHI M"
S11   1849  SELECT AU= "SEKI H" OR AU= "SEKI H."
S12      1  SELECT AU= "SEKI HIDENOBU"
S13   1131  SELECT AU= "SEKI, H" OR AU= "SEKI, H."
S14      1  S AU=(HIDENOBU, S? OR HIDENOBU S?)
S15   4877  S S1:S14
S16   9332  S PASSWORD? ? OR PASSCODE? ? OR PASSPHRASE? ? OR PASS()(WORD? ? OR CODE? ? OR PHRASE? ?)
S17      0  S S15 AND S16
; show files
```

[File 8] **Ei Compendex(R)** 1884-2006/Nov W1
(c) 2006 Elsevier Eng. Info. Inc. All rights reserved.
**File 8: The file has been reprocessed and accession numbers have changed. See HELP NEWS988 for details.*

[File 35] **Dissertation Abs Online** 1861-2006/Nov
(c) 2006 ProQuest Info&Learning. All rights reserved.

[File 65] **Inside Conferences** 1993-2006/Nov 27
(c) 2006 BLDSC all rts. reserv. All rights reserved.

[File 2] **INSPEC** 1898-2006/Nov W3
(c) 2006 Institution of Electrical Engineers. All rights reserved.

[File 94] **JICST-EPlus** 1985-2006/Aug W2
(c)2006 Japan Science and Tech Corp(JST). All rights reserved.

[File 111] **TGG Natl.Newspaper Index(SM)** 1979-2006/Nov 09
(c) 2006 The Gale Group. All rights reserved.

[File 6] **NTIS** 1964-2006/Nov W2
(c) 2006 NTIS, Intl Cpyrght All Rights Res. All rights reserved.

[File 144] **Pascal** 1973-2006/Nov W1
(c) 2006 INIST/CNRS. All rights reserved.

[File 434] **SciSearch(R) Cited Ref Sci** 1974-1989/Dec
(c) 2006 The Thomson Corp. All rights reserved.

[File 34] **SciSearch(R) Cited Ref Sci** 1990-2006/Nov W3
(c) 2006 The Thomson Corp. All rights reserved.

[File 62] **SPIN(R)** 1975-2006/Nov W2
(c) 2006 American Institute of Physics. All rights reserved.

[File 99] **Wilson Appl. Sci & Tech Abs** 1983-2006/Sep
(c) 2006 The HW Wilson Co. All rights reserved.

[File 95] **TEME-Technology & Management** 1989-2006/Nov W4
(c) 2006 FIZ TECHNIK. All rights reserved.

[File 56] **Computer and Information Systems Abstracts** 1966-2006/Nov
(c) 2006 CSA. All rights reserved.

[File 57] **Electronics & Communications Abstracts** 1966-2006/Nov
(c) 2006 CSA. All rights reserved.

[File 60] **ANTE: Abstracts in New Tech & Engineer** 1966-2006/Nov
(c) 2006 CSA. All rights reserved.

[File 266] **FEDRIP** 2006/Aug
Comp & dist by NTIS, Intl Copyright All Rights Res. All rights reserved.

[File 583] **Gale Group Globalbase(TM)** 1986-2002/Dec 13
(c) 2002 The Gale Group. All rights reserved.
**File 583: This file is no longer updating as of 12-13-2002.*

[File 438] **Library Lit. & Info. Science** 1984-2006/Sep
(c) 2006 The HW Wilson Co. All rights reserved.

Keyword - Patent, fulltext

Set	Items	Description
S1	41230	S PASSWORD? ? OR PASSCODE? ? OR PASSPHRASE? ? OR PASS()(WORD? ? OR CODE? ? OR PHRASE? ?)
S2	597875	S PIN OR PINS OR CREDENTIAL? ?
S3	524801	S MATCH?? OR MATCHING
S4	3462	S S1 (5N) (BREAK??? OR BROKEN OR IDENTIFY OR IDENTIFIED OR DISCOVER?? OR (FOUND OR FIND)()OUT OR DETERMINE? ? OR ASCERTAIN?? OR GUESS?? OR DEDUCE? ? OR (WORK OR FIGURE OR FIND)()OUT OR DISCOVER?? OR DETERMINE? ? OR STOLEN OR STEAL OR EXTORT?? OR ATTACK??)
S5	1970	S S1 (5N) S3
S6	2111	S S1 (3N) (GENERATED OR AUTOMAT? OR CANDIDATE? ? OR RANDOM)
S7	135	S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL) (3W) S6
S8	8	S S7 (7N) (PERIOD? OR DURATION? ? OR TIME)

```
S9        8  IDPAT (sorted in duplicate/non-duplicate order)
S10       8  IDPAT (primary/non-duplicate records only)
S11       7  S S7 (7N) (S4 OR S5)
S12       7  S S11 NOT S10
S13       7  IDPAT (sorted in duplicate/non-duplicate order)
S14       7  IDPAT (primary/non-duplicate records only)
S15     189  S (S4 OR S5) (5N) (PERIOD? OR DURATION? ? OR TIME OR HOW()(LONG OR FAST OR QUICK??) )
S16    5598  S S1 (5N) (STRENGTH OR STRONG?? OR GOOD OR HIGH()QUALITY OR INTENSITY OR RESISTANCE OR
VULNERABL? ? OR SECURE OR SECURITY)
S17      17  S S15 (30N) S16
S18      17  S S17 NOT (S10 OR S14)
S19      10  S S18 AND AY=1963:2002
S20      10  IDPAT (sorted in duplicate/non-duplicate order)
S21       7  IDPAT (primary/non-duplicate records only)
S22 1365141  S COMBINATION? ? OR PERMUTATION? ?
S23   17622  S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL) (3W) S22
S24     440  S S1 (3N) (PRODUCE? ? OR CONSTRUCT?? OR BUILT OR PREPARE? ? )
S25     150  S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL) (3W) (S24 OR S6)


S26     326  S (S25 OR S23) (10N) (RATIO OR RATIOS OR PERCENTAGE? ?)
S27       0  S S25 (10N) S23 (10N) (RATIO OR RATIOS OR PERCENTAGE? ?)
S28       0  S S26 (30N) S16
S29     144  S S23 (30N) S1
S30       0  S (S25 OR S29) (10N) (RATIO OR RATIOS OR PERCENTAGE? ?)
S31       3  S S25 (30N) S29
S32       2  S S31 NOT (S10 OR S14 OR S21)
S33     559  S S1 (3N) (PROPOSED OR POSSIBLE? ? OR POTENTIAL? ? OR VIABLE? ? OR FEASIBLE OR FEASIBILITIES
OR POSSIBILITIES )
S34       0  S S33 (10N) (S24 OR (GENERATED (3N) S1)) (10N) (RATIO OR RATIOS OR PERCENTAGE? ? )
S35      15  S S33 (30N) (S24 OR (GENERATED (3N) S1))
S36      15  S S35 NOT (S10 OR S14 OR S21)
S37      15  IDPAT (sorted in duplicate/non-duplicate order)
S38      11  IDPAT (primary/non-duplicate records only)
S39       9  S S38 AND AY=1963:2002
; show files
```

[File 348] **EUROPEAN PATENTS** 1978-2006/ 200646
(c) 2006 European Patent Office. All rights reserved.
**File 348:* *For important information about IPCR/8 and forthcoming changes to the IC= index, see HELP NEWSIPCR.*

[File 349] **PCT FULLTEXT** 1979-2006/UB=20061123UT=20061116
(c) 2006 WIPO/Thomson. All rights reserved.
**File 349:* *For important information about IPCR/8 and forthcoming changes to the IC= index, see HELP NEWSIPCR.*

[File 350] **Derwent WPIX** 1963-2006/UD=200675
(c) 2006 The Thomson Corporation. All rights reserved.
**File 350:* *DWPI has been enhanced to extend content and functionality of the database. For more info, visit http://www.dialog.com/dwpi/.*

Wrong date

10/5,K/1 (Item 1 from file: 350)
Derwent WPIX
(c) 2006 The Thomson Corporation. All rights reserved.

0015299112 *Drawing available*
WPI Acc no: 2005-649286/200566
XRPX Acc No: N2005-531883
One time password calculation method in hardware device for authenticating user, involves concatenating secret uniquely assigned to token, with count that increases monotonically at token and authentication server
Patent Assignee: VERISIGN INC (VERI-N)
Inventor: POPP N

Patent Family (1 patents, 107 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
WO 2005083610	A1	20050909	WO 2005US5481	A	20050223	200566	B

Priority Applications (no., kind, date): US 2004546194 P 20040223

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
WO 2005083610	A1	EN	19	2		
National Designated States,Original	AE AG AL AM AT AU AZ BA BB BG BR BW BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE EG ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NA NI NO NZ OM PG PH PL PT RO RU SC SD SE SG SK SL SM SY TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW					
Regional Designated States,Original	AT BE BG BW CH CY CZ DE DK EA EE ES FI FR GB GH GM GR HU IE IS IT KE LS LT LU MC MW MZ NA NL OA PL PT RO SD SE SI SK SL SZ TR TZ UG ZM ZW					

Alerting Abstract WO A1
NOVELTY - A secret uniquely assigned to token and shared between token and authentication server, is concatenated with a count that increases monotonically at token, with **number** of one **time passwords** (OTOs) **generated** at token and increases monotonically at server, with each calculation of the OTP at server. A hash is calculated using concatenated secret and count. The OTP is obtained by truncating the result of the hash.

DESCRIPTION - An INDEPENDENT CLAIM is also included for method for authenticating request for access to resource.
USE - For calculating one time passwords (OTPs) in hardware device used to verify identity of user and authenticate user for deciding whether to grant request for access to data or services in network.
ADVANTAGE - The OTPs are generated by a token that includes mechanisms to prevent the unauthorized modification or disclosure of the software and information and to help ensure its proper functioning.
DESCRIPTION OF DRAWINGS - The figure shows a sequence diagram explaining the authentication procedure.

Title Terms /Index Terms/Additional Words: ONE; TIME; PASSWORD; CALCULATE; METHOD; HARDWARE; DEVICE; AUTHENTICITY; USER; SECRET; UNIQUE; ASSIGN; TOKEN; COUNT; INCREASE; MONOTONIC; SERVE

Class Codes

International Patent Classification

IPC	**Class Level**	**Scope**	**Position**	**Status**	**Version Date**
G06F-017/60			Main		"Version 7"

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-E04; T01-N02B1B

...NOVELTY - A secret uniquely assigned to token and shared between token and authentication server, is concatenated with a count that increases monotonically at token, with **number** of one **time passwords** (OTOs) **generated** at token and increases monotonically at server, with each calculation of the OTP at server. A hash is calculated using concatenated secret and count. The...

Original Publication Data by Authority

...
Original Abstracts:
secret can be a private key or a shared secret symmetric key. The count is a number that increases monotonically at the token with the **number** of one-**time Passwords generated** at the token. The count is also tracked at an authentication server, where it increases monotonically with each calculation of a one-time Password at...

Wrong date

10/5K/6 (Item 6 from file: 349)
PCT FULLTEXT
(c) 2006 WIPO/Thomson. All rights reserved.
01408341
APPARATUS FOR INPUTTING PASSWORD AND METHOD OF INPUTTING AND DECRYPTING PASSWORD
APPAREIL POUR ENTRER UN MOT DE PASSE, PROCEDE POUR ENTRER ET DECRYPTER UN MOT DE PASSE

Patent Applicant/Patent Assignee:

- **SORINAMOO MEDIA CO LTD**; 4 floor, Jiyoung building annex, Nonhyeon-dong 215-1, Kangnam-gu, Seoul 135-829
  KR; KR (Residence); KR (Nationality)
  (For all designated states except: US)
- **IM Byung-ryul**; Daesung mansion apartment 201ho, Bangi-dong 159, Songpa-gu, Seoul 138-050
  KR; KR (Residence); KR (Nationality)
  (Designated only for: US)

Patent Applicant/Inventor:

- **IM Byung-ryul**
  Daesung mansion apartment 201ho, Bangi-dong 159, Songpa-gu, Seoul 138-050; KR; KR (Residence); KR (Nationality); (Designated only for: US)

Legal Representative:

- **HWANG Sung-tag(agent)**
  Ka-4410, Chungang circulation complex, 1258 Kurobon-dong, Kuro-gu, Seoul 152-059; KR;

	Country	Number	Kind	Date
Patent	WO	200691001	A1	20060831
Application	WO	2006KR585		20060221

Priorities	KR	1020050016338		20050228
	KR	1020050040016		20050513
	KR	1020050053799		20050622
	KR	1020050068767		20050728

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)
AE; AG; AL; AM; AT; AU; AZ; BA; BB; BG;
BR; BW; BY; BZ; CA; CH; CN; CO; CR; CU;
CZ; DE; DK; DM; DZ; EC; EE; EG; ES; FI;
GB; GD; GE; GH; GM; HR; HU; ID; IL; IN;
IS; JP; KE; KG; KM; KN; KP; KZ; LC; LK;
LR; LS; LT; LU; LV; LY; MA; MD; MG; MK;
MN; MW; MX; MZ; NA; NG; NI; NO; NZ; OM;
PG; PH; PL; PT; RO; RU; SC; SD; SE; SG;
SK; SL; SM; SY; TJ; TM; TN; TR; TT; TZ;
UA; UG; US; UZ; VC; VN; YU; ZA; ZM; ZW;

[EP] AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES;
FI; FR; GB; GR; HU; IE; IS; IT; LT; LU;
LV; MC; NL; PL; PT; RO; SE; SI; SK; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW;
ML; MR; NE; SN; TD; TG;

[AP] BW; GH; GM; KE; LS; MW; MZ; NA; SD; SL;
SZ; TZ; UG; ZM; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

IPC	Level	Value	Position	Status	Version	Action	Source	Office
G06F-0015/00	A	I	F	B	20060101		H	KR

Publication Language:	English
Filing Language:	English
Fulltext word count:	12085

English Abstract:

The present invention relates to an apparatus for inputting a password and a method of inputting and decrypting a password. An original password (40) is composed of a password frame (42), an operator frame (44) and a shadow frame (46). The password frame is composed of four or more password numerals, and the shadow frame is composed of a number of numerals, which is identical to the number of numerals of the password frame. On a display unit, 10 numbers are randomly written at 10 addresses and displayed. An SPU (30) can recognize that the first numeral of a virtual password is generated by performing an operation on a number at an address corresponding to the first numeral of the password frame and the first numeral of the shadow frame through an operator, and the remaining numerals of the virtual password are generated through the above operation.

French Abstract:

L'invention concerne un appareil pour entrer un mot de passe et un procede pour entrer et decrypter un mot de passe. Un mot de passe original (40) est compose d'une trame de mot de passe (42), d'une trame d'operateur (44) et d'une trame de protection (46). La trame de mot de passe est composee de quatre elements numeraux ou plus, et la trame de protection est composee d'un certain nombre d'elements numeraux, identique au nombre des elements numeraux de la trame de mot de passe. Sur une unite d'affichage, dix chiffres sont ecrits au hasard dans dix adresses et ils sont affiches. Une unite processeur secret (SPU) (30) peut reconnaitre si le premier element numeral d'un mot de passe virtuel est genere par une operation executee sur un chiffre d'une adresse correspondant au premier element numeral de la trame de mot de passe et au premier element numeral de la trame de protection par un operateur, les elements numeraux restants du mot de passe virtuel etant generes par cette operation.

Type	Pub. Date	Kind	Text
Publication	20060831	A1	With international search report.

Detailed Description:

...SPU performs an inverse operation on condition values of the display window, which are addresses indicating whether to use a token value, and an arbitrary **number** added to the **generated** one- **time password**, thus generating values 1SS8. Through such a method, the SPU determines whether a virtual password, decrypted based on in-formation indicating whether the one-time...

Wrong date

10/5K/7 (Item 7 from file: 349)
PCT FULLTEXT
(c) 2006 WIPO/Thomson. All rights reserved.
01276112
TOKEN AUTHENTICATION SYSTEM AND METHOD
SYSTEME ET PROCEDE D'AUTHENTIFICATION DE JETONS

Patent Applicant/Patent Assignee:

- **VERISIGN INC**; 487 East Middlefield Road, Mountain View, CA 94043
  US; US (Residence); US (Nationality)
  (For all designated states except: US)

- **POPP Nicolas**; 196 Santa Monica Ave., Menlo Park, CA 94025
  US; US (Residence); US (Nationality)
  (Designated only for: US)

Patent Applicant/Inventor:

- **POPP Nicolas**
  196 Santa Monica Ave., Menlo Park, CA 94025; US; US (Residence); US (Nationality); (Designated only for: US)

Legal Representative:

- **ROSINI James E et al(agent)**
  Kenyon & Kenyon, 1500 K Street, N.W., Suite 700, Washington, DC 20005; US;

	Country	Number	Kind	Date
Patent	WO	200583610	A1	20050909
Application	WO	2005US5481		20050223
Priorities	US	2004546194		20040223

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)
AE; AG; AL; AM; AT; AU; AZ; BA; BB; BG;
BR; BW; BY; BZ; CA; CH; CN; CO; CR; CU;
CZ; DE; DK; DM; DZ; EC; EE; EG; ES; FI;
GB; GD; GE; GH; GM; HR; HU; ID; IL; IN;
IS; JP; KE; KG; KP; KR; KZ; LC; LK; LR;
LS; LT; LU; LV; MA; MD; MG; MK; MN; MW;
MX; MZ; NA; NI; NO; NZ; OM; PG; PH; PL;
PT; RO; RU; SC; SD; SE; SG; SK; SL; SM;
SY; TJ; TM; TN; TR; TT; TZ; UA; UG; US;
UZ; VC; VN; YU; ZA; ZM; ZW;

[EP] AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES;
FI; FR; GB; GR; HU; IE; IS; IT; LT; LU;
MC; NL; PL; PT; RO; SE; SI; SK; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW;
ML; MR; NE; SN; TD; TG;

[AP] BW; GH; GM; KE; LS; MW; MZ; NA; SD; SL;
SZ; TZ; UG; ZM; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Main International Patent Classes (Version 7):

IPC	**Level**
G06F-017/60	Main
Publication Language:	English
Filing Language:	English
Fulltext word count:	4194

English Abstract:

A method for calculating a One Time Password. A secret is concatenated with a count, where the secret is uniquely assigned to a token. The secret can be a private key or a shared secret symmetric key. The count is a number that increases monotonically at the token with the **number** of one-**time Passwords generated** at the token. The count is also tracked at an authentication server, where it increases monotonically with each calculation of a one-time Password at the authentication server. An OTP can be calculated by hashing a concatenated secret and count. The result can be truncated.

English Abstract:

...secret can be a private key or a shared secret symmetric key. The count is a number that increases monotonically at the token with the **number** of one-**time Passwords generated** at the token. The count is also tracked at an authentication server, where it increases monotonically with each calculation of a one-time Password at...

French Abstract:

procede de calcul d'un mot de passe a usage unique. Un secret est concatene avec un compte, le secret etant specifiquement attribue a un jeton. Le secret peut etre une cle prive ou une cle symetrique secrete partagee. Le compte est un nombre a croissance monotone au niveau du jeton avec le nombre de mots de passe a usage unique generes dans le jeton. De plus, ce compte est suivi par un serveur

d'authentification et croit monotonement a chaque calcul d'un mot de passe unique dans le serveur d'authentification. Un mot de passe a usage unique peut egalement etre calcule par hachage d'un secret et d'un compte concatene. Le resultat peut etre tronque.

Type	Pub. Date	Kind	Text
Publication	20050909	A1	With international search report.
Publication	20050909	A1	Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Correction	20060921		Corrections of entry in Section 1:
Republication	20060921	A1	With international search report.

Detailed Description:

...secret can be a private key or a shared secret symmetric key. The count is a number that increases monotonically at the token with the **number** of One **Time Passwords generated** at the token. The count is also tracked at an authentication server, where it increases monotonically with each calculation of a One Time Password at...

Claims:

...token and is shared between the token and an authentication server, and the count is a number that increases monotonically at the token with the **number** of One **Time Passwords generated** at the token and increases monotonically at the authentication server with each calculation at the authentication server of a One Time Password;
calculating a hash...

Wrong date

14/5,K/1 (Item 1 from file: 350)
Derwent WPIX
(c) 2006 The Thomson Corporation. All rights reserved.

0015104098 *Drawing available*
WPI Acc no: 2005-453575/200546
Method for managing password on internet and computer device for executing the same
Patent Assignee: KIM H S (KIMH-I); YOON J W (YOON-I)
Inventor: KIM H S; YOON J W

Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
KR 2005017031	A	20050221	KR 200355395	A	20030811	200546	B

Priority Applications (no., kind, date): KR 200355395 A 20030811

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes
KR 2005017031	A	KO	1	10	

Alerting Abstract KR A
NOVELTY - A method for managing a password on the Internet and a computer device for executing the same are provided to safely manage multiple passwords used to each web site by using one master password.
DESCRIPTION - A **random number password** generator generates a temporary **password** of a random number **matched** with a name of each web site inputted from a user. A real password generator generates a real password for each web site by encoding the

unique master password inputted from the user with the temporary password as a key value. A means manages a login ID/password used for logging in to a password management computing device.

Title Terms /Index Terms/Additional Words: METHOD; MANAGE; PASSWORD; COMPUTER; DEVICE; EXECUTE

Class Codes

International Patent Classification

IPC	**Class Level**	**Scope**	**Position**	**Status**	**Version Date**
G06F-015/00			Main		"Version 7"

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-J

Alerting Abstract DESCRIPTION - A **random number password** generator generates a temporary **password** of a random number **matched** with a name of each web site inputted from a user. A real password generator generates a real password for each web site by encoding...

Your application

14/5,K/2 (Item 2 from file: 350)
Derwent WPIX
(c) 2006 The Thomson Corporation. All rights reserved.

0014143953 *Drawing available*
WPI Acc no: 2004-328733/
XRPX Acc No: N2004-262269
Password strength checking method involves generating next password candidate when input password does not match with generated plaintext password candidate, and calculating number of candidates when match is determined
Patent Assignee: YAMATAKE CORP (YAMA-N); YAMATAKE HONEYWELL CO LTD (HONF)
Inventor: ARIMOTO M; ARIMOTO N; MISHIMA T; SANAI D; SEKI E; SEKI H

Patent Family (4 patents, 2 countries)

Patent Number	**Kind**	**Date**	**Application Number**	**Kind**	**Date**	**Update**	**Type**
US 20040073815	A1	20040415	US 2003677277	A	20031003	200430	B
JP 2004133720	A	20040430	JP 2002298190	A	20021011	200430	E
JP 2004199320	A	20040715	JP 2002366243	A	20021218	200446	E
JP 2004199322	A	20040715	JP 2002366258	A	20021218	200446	E

Priority Applications (no., kind, date): JP 2002366258 A 20021218; JP 2002298190 A 20021011; JP 2002366243 A 20021218

Patent Details

Patent Number	**Kind**	**Lan**	**Pgs**	**Draw**	**Filing Notes**	
US 20040073815	A1	EN	47	31		
JP 2004133720	A	JA	13			
JP 2004199320	A	JA	16			

JP 2004199322	A	JA	11			

Alerting Abstract US A1
NOVELTY - A plaintext password candidate is generated according to generation procedure same as the procedure used by a password guessing tool. The next password candidate is generated when the input password does not match with the generated password candidate. The strength of the input **password** is **determined** based on the **number** of the **generated password candidates** when the **match** is **determined**.
DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

11. a password strength checking apparatus;

12. a program for checking password strength;

13. a recorded medium storing password strength checking program;

14. a password creation assisting method;

15. a program for assisting password creation;

16. password creation method; and

17. a password creating program.

USE - For checking strength of password for access approval of computer system used in office.
ADVANTAGE - The password strength can be calculated in practical duration of time, thereby enabling accurate checking of the password strength and enhancing security for internal information.
DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the password strength checking apparatus.

Title Terms /Index Terms/Additional Words: PASSWORD; STRENGTH; CHECK; METHOD; GENERATE; CANDIDATE; INPUT; MATCH; CALCULATE; NUMBER; DETERMINE

Class Codes

International Patent Classification

IPC	Class Level	Scope	Position	Status	Version Date
G06F-015/00; H04L-009/00			Main		"Version 7"
H04L-009/32			Secondary		"Version 7"

US Classification, Issued: 713202000

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-N02B1B; T01-S03

...guessing tool. The next password candidate is generated when the input password does not match with the generated password candidate. The strength of the input **password** is **determined** based on the **number** of the **generated password candidates** when the **match** is **determined**.

Original Publication Data by Authority

...

Original Abstracts:

or not the inputted password and the generated password candidate match each other, directing generation of the next password candidate when the match is not **determined**, determining strength of the inputted **password** based on the **number** of the **generated password candidates** when the **match** is **determined**, and outputting information of the determined password strength.

...

Claims:

or not the inputted password and the generated password candidate match each other;directing generation of the next password candidate when the match is not **determined**;determining strength of the inputted **password** based on the **number** of the **generated password candidates** when the **match** is **determined**; andoutputting information of **the determined** password strength.

21/5K/3 (Item 3 from file: 349)
PCT FULLTEXT
(c) 2006 WIPO/Thomson. All rights reserved.
00870979

INFORMATION RECORD INFRASTRUCTURE, SYSTEM AND METHOD
INFRASTRUCTURE DE DOSSIERS D'INFORMATION, ET SYSTEME ET PROCEDE ASSOCIES

Patent Applicant/Inventor:

- **FELSHER David Paul**
  158 Blackhouse Road, Trumbull, CT 06611; US; US(Residence); US(Nationality);

Legal Representative:

- **HOFFBERG Steven M(agent)**
  Milde, Hoffberg & Macklin, LLP, Suite 460, 10 Bank Street, White Plains, NY 10606; US;

	Country	Number	Kind	Date
Patent	WO	200205061	A2-A3	20020117
Application	WO	2001US21234		20010705
Priorities	US	2000216199		20000706
	US	2000223246		20000804

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

[EP] AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;
GR; IE; IT; LU; MC; NL; PT; SE; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GW; ML;
MR; NE; SN; TD; TG;

[AP] GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ;
UG; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Main International Patent Classes (Version 7):

IPC	Level

H04L-009/00	Main
H04L-009/32	
Publication Language:	English
Filing Language:	English
Fulltext word count:	19890

English Abstract:

A method of maintaining digital medical records, comprising a step of receiving a medical transaction record (102), encrypted with a key in accordance with a patient-file association. Also comprising a step of accessing the encrypted medical transaction record according to a patient association with the record (111). And further comprising a step of re-encryption of the encrypted accessed medical transaction record with a key associated with an intended recipient of the medical record. The system and method according to the present invention presents a new business model for creation, maintenance, transmission, and use of medical records. The invention also allows financial burdens to be reallocated optimally and equitably, resulting in decreased overall societal cost and providing a successful business model for a database proprietor. Secure entrusted medical records are held in trust by an independent third party on behalf of the patient (113), and serve the medical community at large. Separately encrypted record elements may be aggregated as an information polymer.

French Abstract:

L'invention porte sur un procede de conservation de documents medicaux electroniques comprenant les etapes suivantes: reception d'un dossier d'actes medicaux crypte a l'aide d'un code associe au patient, acces audit dossier au moyen du code associe au patient, et nouveau cryptage du dossier a l'aide d'un code associe au destinataire prevu du dossier. Le systeme et le procede de l'invention constituent un nouveau modele d'affaires servant a la creation, la gestion, la transmission, et l'utilisation de dossiers medicaux, et permettant de reventiler les charges financieres, par exemple mieux et plus equitablement, pour faire baisser les couts sociaux globaux, ou permettant simplement de constituer un modele d'affaires pour proprietaires de bases de donnees. Les dossiers sont confies en toute securite a un tiers independant agissant pour le compte du patient et servant la communaute medicale dans son ensemble. De plus, les elements des dossiers cryptes separement peuvent etre reunis sous la forme d'un agregat d'informations.

Type	Pub. Date	Kind	Text
Publication	20020117	A2	Without international search report and to be republished upon receipt of that report.
Examination	20020606		Request for preliminary examination prior to end of 19th month from priority date
Search Rpt	20020704		Late publication of international search report
Republication	20020704	A3	With international search report.

Detailed Description:

...the currently displayed password from the SecurID device. This information is transmitted to a security server, which authenticates the user and verifies that, the correct **password** was entered. The **security** server compares the user-entered **password** with. its knowledge of what: password should have been entered for that 60 second **period**. If the **password** does not **match**, it also checks the **password** from the previous 60 second **period** to account for delays in typing and transmission. Once a password is verified, the user is authenticated for the duration of the session, or possibly...

21/5K/6 (Item 6 from file: 349)
PCT FULLTEXT
(c) 2006 WIPO/Thomson. All rights reserved.
00460571

METHOD AND SYSTEM FOR ACCESSING ELECTRONIC RESOURCES VIA MACHINE-READABLE DATA ON INTELLIGENT DOCUMENTS

PROCEDE ET SYSTEME D'ACCES A DES RESSOURCES ELECTRONIQUES PAR L'INTERMEDIAIRE DE DONNEES EXPLOITABLES PAR MACHINE SUR DOCUMENTS INTELLIGENTS

Patent Applicant/Patent Assignee:

- **NEOMEDIA TECHNOLOGIES INC**;
  ; ;
- **DURST Robert T Jr**;
  ; ;
- **HUNTER Kevin**;
  ; ;

	Country	Number	Kind	Date
Patent	WO	9851035	A1	19981112
Application	WO	98US9441		19980509
Priorities	US	9746037		19970509
	US	97967383		19971108
	US	9823918		19980213

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

Main International Patent Classes (Version 7):

IPC	Level
H04L-009/00	Main
H04L-07:32	
H04N-01:40	
H03M-07:30	
G06F-15:40	
Publication Language:	English
Filing Language:	
Fulltext word count:	8146

English Abstract:

A method of accessing electronic resources via machine readable data embedded on a document which comprises compressing input data with a transmitter adapted to save a first bandwidth using a compression method adapted to minimize utilization of bandwidth by the compressed input data while retaining substantially all information content of the input data and appending a compression flag to the compressed input data indicative of the compression method enabling a receiver to decompress the compressed input data. The compression step further comprises utilizing a compression dictionary adapted to map the elements and strings of the input data to minimized representations having redundancies deleted. The compression dictionary may be appended to the compressed input data (as cleartext or cyphertext) under circumstances where a bandwidth occupied by the appended compression dictionary is less than the bandwidth saved by the step of compressing the input data. The compression dictionary may also be selected by the receiver independently from the transmitter independently indexes, pointer registration, application restricted subsets or customized according to the input data content. Also the input data may be encrypted, and an encryption flag appended which is indicative of the encryption method enabling decryption via public or private key cryptosystems as well as utilizing various authentication techniques such as digital signatures to ensure that the document was created by a licensed user.

French Abstract:

L'invention concerne un procede d'acces a des ressources electroniques par l'intermediaire de donnees exploitables sur machine, ces donnees etant integrees a un document. Ce procede consiste a comprimer des donnees d'entree par l'intermediaire d'un emetteur, concu pour sauvegarder une premiere largeur de bande grace a un procede de compression. Ce procede permet de minimiser l'utilisation de cette largeur de bande par lesdites donnees d'entree comprimees, tout en conservant sensiblement tout le contenu de ces donnees d'entree et en ajoutant un indicateur de compression a ces donnees, afin d'indiquer le procede de compression permettant a un recepteur de decomprimer ces donnees d'entree comprimees. Cette etape de compression consiste ensuite a utiliser un dictionnaire de

compression, concu pour faire correspondre les elements et les chaines de caractere des donnees d'entree a des representations de taille inferieure, dont les redondances ont ete effacees. On peut ajouter ce dictionnaire de compression audites donnees d'entree comprimees (en tant que texte en clair ou chiffre), si la largeur de bande occupee par le dictionnaire de compression est inferieure a celle sauvegardee au cours de l'etape de compression des donnees d'entree. Ce dictionnaire de compression peut egalement etre choisi par le recepteur, independamment des indices, de l'enregistrement du pointeur, des sous-ensembles limites a une application, ou personnalise en fonction du contenu desdites donnees d'entree. Celles-ci peuvent en outre etre chiffrees, et un indicateur de compression ajoute, afin d'indiquer le procede de chiffrement suivi, ce qui permet un dechiffrement par des systemes de chiffrement a cle publique ou privee, ainsi que l'utilisation de diverses techniques d'authentification telles que des signatures numeriques, qui permettent de s'assurer que le document a ete cree par un utilisateur autorise.

Detailed Description:

...With any static password based authentication mechanism selection of the password should be undertaken to provide immunity to guessing and dictionary attack. However, when a **secure password** is entered in cleartext over an unsecure channel, it is as subject to network eavesdropping as an unsecure password.

An alternative scheme that prevents such **attacks** is a one-**time password** system. Unlike authentication mechanisms based on static passwords, those based on one-time passwords are not at all endangered by cleartext password entry. Three popular...

32/5K/1 (Item 1 from file: 349)
PCT FULLTEXT
(c) 2006 WIPO/Thomson. All rights reserved.
01435738
IMAGING DEVICE AND DRIVE RECORDER SYSTEM
DISPOSITIF D'IMAGERIE ET SYSTEME ENREGISTREUR DE CONDUITE

Patent Applicant/Patent Assignee:

- **NIKON CORPORATION**; 2-3, Marunouchi 3-Chome, Chiyoda-ku, Tokyo, 1008331
  JP; JP (Residence); JP (Nationality)
  (For all designated states except: US)
- **FUJINAWA Nobuhiro**; C/O NIKON CORPORATION, Intellectual Property Department, 2-3, Marunouchi 3-Chome, Chiyoda-ku, Tokyo, 1008331
  JP; JP (Residence); JP (Nationality)
- **NOZAKI Hirotake**; C/O NIKON CORPORATION, Intellectual Property Department, 2-3, Marunouchi 3-Chome, Chiyoda-ku, Tokyo, 1008331
  JP; JP (Residence); JP (Nationality)
- **MITSUHASHI Setsu**; C/O NIKON CORPORATION, Intellectual Property Department, 2-3, Marunouchi 3-Chome, Chiyoda-ku, Tokyo, 1008331
  JP; JP (Residence); JP (Nationality)

Patent Applicant/Inventor:

- **FUJINAWA Nobuhiro**
  C/O NIKON CORPORATION, Intellectual Property Department, 2-3, Marunouchi 3-Chome, Chiyoda-ku, Tokyo, 1008331; JP;
  JP (Residence); JP (Nationality);

- **NOZAKI Hirotake**
  C/O NIKON CORPORATION, Intellectual Property Department, 2-3, Marunouchi 3-Chome, Chiyoda-ku, Tokyo, 1008331; JP;
  JP (Residence); JP (Nationality);

- **MITSUHASHI Setsu**
  C/O NIKON CORPORATION, Intellectual Property Department, 2-3, Marunouchi 3-Chome, Chiyoda-ku, Tokyo, 1008331; JP;
  JP (Residence); JP (Nationality);

Legal Representative:

- **FURUYA Fumio et al(agent)**
  Dai2 Meiho Bldg. 9th Floor, 19-5, Nishishinjuku 1-Chome, Shinjuku-ku, Tokyo, 1600023; JP;

	Country	Number	Kind	Date
Patent	WO	2006120911	A1	20061116
Application	WO	2006JP308770		20060426
Priorities	JP	2005136052		20050509

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)
AE; AG; AL; AM; AT; AU; AZ; BA; BB; BG;
BR; BW; BY; BZ; CA; CH; CN; CO; CR; CU;
CZ; DE; DK; DM; DZ; EC; EE; EG; ES; FI;
GB; GD; GE; GH; GM; HR; HU; ID; IL; IN;
IS; KE; KG; KM; KN; KP; KR; KZ; LC; LK;
LR; LS; LT; LU; LV; LY; MA; MD; MG; MK;
MN; MW; MX; MZ; NA; NG; NI; NO; NZ; OM;
PG; PH; PL; PT; RO; RU; SC; SD; SE; SG;
SK; SL; SM; SY; TJ; TM; TN; TR; TT; TZ;
UA; UG; US; UZ; VC; VN; YU; ZA; ZM; ZW;

[EP] AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES;
FI; FR; GB; GR; HU; IE; IS; IT; LT; LU;
LV; MC; NL; PL; PT; RO; SE; SI; SK; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW;
ML; MR; NE; SN; TD; TG;

[AP] BW; GH; GM; KE; LS; MW; MZ; NA; SD; SL;
SZ; TZ; UG; ZM; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

IPC	Level	Value	Position	Status	Version	Action	Source	Office
H04N-0005/915	A	I	F	B	20060101		H	JP
B62D-0041/00	A	I	L	B	20060101		H	JP
H04N-0005/225	A	I	L	B	20060101		H	JP
B60R-0021/00	A	N	L	B	20060101		H	JP

Publication Language: Japanese

Filing Language: Japanese
Fulltext word count: 27731

English Abstract:

An imaging device mounted on a vehicle and imaging the periphery of the vehicle, the imaging device having an imaging lens, an imaging element, an accident detection sensor, an image processing section, and a recording section. The imaging element creates an image signal by photoelectrically converting a field image that is based on a light flux from the imaging lens. The accident detection sensor detects the occurrence of an accident based on an impact on the vehicle. When an accident occurs, the image processing section creates, based on the image signal, first accident image data and second accident image data where the situation of the same accident is stored. The recording section records both the first accident image data and second accident image data individually in conditions where security levels relative to data reliability are different.

French Abstract:

L'invention concerne un dispositif d'imagerie monte sur un vehicule et prenant la peripherie du vehicule, le dispositif d'imagerie possedant une lentille d'imagerie, un element d'imagerie, un detecteur d'accident, une section de traitement d'image et une section d'enregistrement. L'element d'imagerie cree un signal image en convertissant par photoelectricite une image de champ basee sur un flux lumineux de la lentille d'imagerie. Le detecteur d'accident detecte l'occurrence d'un accident d'apres l'impact sur le vehicule. Lorsqu'un accident se produit, la section de traitement d'image cree, en fonction du signal image, des premieres donnees d'image d'accident et des deuxiemes donnees d'image d'accident ou est stocke l'emplacement du meme accident. La section d'enregistrement enregistre individuellement a la fois les premieres donnees d'image d'accident et les deuxiemes donnees d'image d'accident dans des conditions ou les niveaux de securite sur le plan de la fiabilite des donnees sont differents.

Type	Pub. Date	Kind	Text
Publication	20061116	A1	With international search report.

Detailed Description:

...are: BCs and the number of BCs per CU are selected in a way convenient to USER to read and reproduce at the time of **Password**/Encryption key generation. The number of CUs in a VCS is selected, ensuring the resulting **number of permutations** of CUs forming unique VCSs and the **total number** of **Passwords**/Encryption keys **generated** from the VCS meets the requirement of USER and SERVICE PROVIDER. The mathematical relationship between BCs, CUs, 445 VCS, Passwords/Encryption keys and PSI is...

39/5K/1 (Item 1 from file: 348)
EUROPEAN PATENTS
(c) 2006 European Patent Office. All rights reserved.
02033520
Play extension system
System zur Spielerweiterung
Systeme pour extension des jeux

Patent Assignee:

- **Konami Corporation**; (3072830)
  3-1, Toranomon 4-chome; Minato-ku,Tokyo; (JP)
  (Applicant designated States: all)

Inventor:

- **Yamaguchi, Takashi**
  c/o Konami Corporation3-1, Toranomon 4-chome; Minato-kuTokyo; (JP)

- **Saeki, Kazuyuki**
  c/o Konami Corporation3-1, Toranomon 4-chome; Minato-kuTokyo; (JP)

Legal Representative:

- **Haley, Stephen (79721)**
  Gill Jennings & Every LLP Broadgate House 7 Eldon Street; London EC2M 7LH; (GB)

	Country	Number	Kind	Date	
Patent	EP	1634630	A1	20060315	(Basic)
Application	EP	2005026331		20011123	
Priorities	JP	2001171663		20010606	
	JP	2001208268		20010709	

Designated States:
DE; GB;

Related Parent Numbers: Patent (Application):EP 1264623 (EP 2001309873)

IPC	Level	Value	Position	Status	Version	Action	Source	Office
A63H-0017/36	A	I	F	B	20060101	20060123	H	EP
A63H-0030/04	A	I	L	B	20060101	20060123	H	EP
A63F-0013/00	A	I	L	B	20060101	20060123	H	EP

Abstract EP 1634630 A1

The present invention provides a play extension system enhancing a fun of a toy system by use of network. The play extension system (SY2) is used by combination with the toy system (SY1) in which a user can change the setting of parameters affecting motion control of a driving machine (1), for extending a playing method with the toy system (SY1). In the system (SY2), the setting information corresponding to the setting state of the parameters is received from a predetermined user terminal (120) through a network (100), and estimation on the obtained setting information is created by referring to a database (112) which stores the setting information and the information for estimating the setting state correspondingly. The created estimation is transmitted to a predetermined destination through the network (100).

Abstract Word Count: 131
NOTE: NONE
NOTE: Figure number on first page: NONE

Type	Pub. Date	Kind	Text
Application:	20060315	A1	Published application with search report
Examination:	20060315	A1	Date of request for examination: 20051214

Publication: English
Procedural: English
Application: English

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200611	325
SPEC A	(English)	200611	12437
Total Word Count (Document A) 12762			
Total Word Count (Document B) 0			
Total Word Count (All Documents) 12762			

Specification: ...beginner cannot operate it well.

Therefore, on the side of a provider, the operating characteristic is estimated on every setting state specified by all the **possible passwords**, and the setting database 112 is built for storing information of estimation so as to be associated with the respective **passwords**. Thus **built** setting database 112 is used for checking the setting state by a user. The estimation information is created as the sentence information for expressing the...

39/5K/6 (Item 6 from file: 348)
EUROPEAN PATENTS
(c) 2006 European Patent Office. All rights reserved.
00527051
A method for generating public and private key pairs using a passphrase.
Verfahren zur Erzeugung von offentlichen und geheimen Schlusselpaaren mittels eines Passwortes.
Procede de generation de paires de cles publiques et secretes utilisant une location de passe.

Patent Assignee:

- **International Business Machines Corporation**; (200120)
  Old Orchard Road; Armonk, N.Y. 10504; (US)
  (applicant designated states: DE;FR;GB;IT;NL)

Inventor:

- **Matyas, Stephen M.**
  10 298 Cedar Ridge Drive; Manassas, VA 22110; (US)
- **Johnson, Donald B.**
  11 635 Crystal Creek Lane; Manassas, VA 22111; (US)
- **Le An V.**
  10 227 Battlefield Drive; Manassas, VA 22110; (US)
- **Martin, William C.**
  1835 Hilliard Lane; Concord, NC 28025; (US)
- **Prymak, Rostislaw**
  15 900 Fairway Drive; Dumfries, VA 22026; (US)
- **Wilkins, John D.**
  P.O. Box 8; Somerville, VA 22739; (US)

Legal Representative:

- **Schafer, Wolfgang, Dipl.-Ing. (62021)**
  IBM Deutschland Informationssysteme GmbH, Patentwesen und Urheberrecht; D-70548 Stuttgart; (DE)

	Country	Number	Kind	Date	
Patent	EP	534420	A2	19930331	(Basic)
	EP	534420	A3	19940608	
Application	EP	92116309		19920911	
Priorities	US	766533		19910927	

Designated States:
DE; FR; GB; IT; NL;

International Patent Class (V7): H04L-009/30; H04L-009/08; **CITED PATENTS: (EP A)**

EP 292790 A; US 4850017 A; EP 202768 A; US 4736423 A; **Abstract** EP 534420 A2

A data processing system, program and method are disclosed for managing a public key cryptographic system which includes a public key, private key pair generator. The method includes the step of generating a first public key, private key pair using a first seed value known to a user, the first seed value being generated from a passphrase. A first random number is generated using the first seed value

and applied to generating the first key pair. The method then generates a first control vector defining a first use of the first public key, private key pair.

The method then continues with the step of generating a second public key, private key pair using a second seed value unknown to the user, the second seed value being a true random number. The second random number is generated using the second seed value in a pseudorandom number generator and applied to generating the second key pair. The method generates a second control vector defining a second use of the second public key, private key pair.

The method then controls the use of the first public key, private key pair using the first control vector and controls the use of the second public key, private key pair with the second control vector. (see image in original document)

Abstract Word Count: 216

Type	Pub. Date	Kind	Text
Application:	19930331	A2	Published application (A1with;A2without)
Change:	19930512	A2	Representative (change)
Examination:	19930908	A2	Date of filing of request for examination: 930716
Change:	19930929	A2	Representative (change)
Search Report:	19940608	A3	Separate publication of the European or International search report
Change:	19940831	A2	Representative (change)
Examination:	19970604	A2	Date of despatch of first examination report: 970418

Refusal:	19981230	A2	Date on which the European patent application was refused: 980814

Publication: English
Procedural: English
Application: English

Available Text	Language	Update	Word Count
CLAIMS A	(English)		1819
SPEC A	(English)		15824
Total Word Count (Document A) 17643			
Total Word Count (Document B) 0			
Total Word Count (All Documents) 17643			

Specification: ...phrase. The passphrase testing 302 may be implemented in the form of a passphrase filter.

The passphrase filter is a routine for rejecting 'bad' user-**constructed passphrases**, i.e., **passphrases** that an adversary might potentially discover by using an exhaustive, directed search. At the time a **potential passphrase** is **generated**, the **passphrase** filter is invoked and the passphrase is provided as a parameter input. Using a dictionary of standard English containing the 10,000 most frequently used...

Keyword - Patent, bib

Set	Items	Description
S1	8618	S PASSWORD? ? OR PASSCODE? ? OR PASSPHRASE? ? OR PASS()(WORD? ? OR CODE? ? OR PHRASE? ?)
S2	498	S S1 (5N) (MATCH?? OR MATCHING)
S3	272	S S1 (5N) (BREAK??? OR BROKEN OR IDENTIFY OR IDENTIFIED OR DISCOVER?? OR (FOUND OR FIND)()OUT OR DETERMINE? ? OR ASCERTAIN?? OR GUESS?? OR DEDUCE? ? OR (WORK OR FIGURE OR FIND)()OUT OR DISCOVER?? OR DETERMINE? ? OR STOLEN OR STEAL OR EXTORT?? OR ATTACK??)
S4	322	S S1 (3N) (GENERATED OR AUTOMAT? OR CANDIDATE? ? OR RANDOM)

```
S5       25   S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL)(3W)S4
S6        2   S S5 (10N) (PERIOD? OR DURATION? ? OR TIME )
S7        0   S S5 (10N) (S2 OR S3)
S8      750   S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL)(3W)S1
S9       68   S S8 (10N) (PERIOD? OR DURATION? ? OR TIME OR S2 OR S3)
S10     302   S S1 (5N) (STRENGTH OR STRONG?? OR GOOD OR HIGH()QUALITY OR INTENSITY OR RESISTANCE OR
VULNERABL? ? OR SECURE OR SECURITY )
S11       3   S S9 AND S10
S12       3   S S11 NOT S6
S13     743   S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL) (3W) (COMBINATION? ? OR
PERMUTATION? ? )
S14       6   S S13 AND S1
S15      38   S S1 (3N)(PROPOSED OR POSSIBLE? ? OR POTENTIAL? ? OR VIABLE? ? OR FEASIBLE OR FEASIBILITIES
OR POSSIBILITIES )
S16   42485   S 1 (3N) (PRODUCE? ? OR CONSTRUCT?? OR BUILT OR PREPARE? ? OR GENERATED)
S17     214   S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL)(3W)(S16 OR S4)
S18  354723   S RATIO OR RATIOS OR PERCENTAGE? ?
S19       4   S S18 (10N) (S14 OR S15 OR S17)
S20       4   S S19 NOT (S6 OR S12)
S21       4   IDPAT (sorted in duplicate/non-duplicate order)
S22       4   IDPAT (primary/non-duplicate records only)
S23       0   S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL) (3W) S15
S24       0   S S23 AND S17
S25       6   IDPAT S14 (sorted in duplicate/non-duplicate order)
S26       6   IDPAT S14 (primary/non-duplicate records only)
S27       6   S S26 NOT (S6 OR S12 OR S22)
; show files
```

[File 347] **JAPIO** Dec 1976-2006/Jul(Updated 061116)
(c) 2006 JPO & JAPIO. All rights reserved.

Wrong date

12/5/1
JAPIO
(c) 2006 JPO & JAPIO. All rights reserved.
07584788 **Image available**
ELECTRONIC LOCK DEVICE

Pub. No.: 2003-078631 [JP 2003078631 A]
Published: March 14, 2003 (20030314)
Inventor: JIN OSAMU
KIKUCHI AKIHIRO
Applicant: DAITO COMMUNICATION APPARATUS CO LTD
Application No.: 2001-267713 [JP 2001267713]
Filed: September 04, 2001 (20010904)
International Class: H04M-011/00; E05B-049/00; H04L-009/32; H04Q-009/00; H04Q-009/12

ABSTRACT

PROBLEM TO BE SOLVED: To provide an electronic lock device, with which unlocking is remotely enabled by using a telephone set and **security** can be improved.

SOLUTION: The **password** number for unlocking of (m) digits is inputted to extension telephone sets 31-3n and a password signal for unlocking is outputted. When the instruction signal part of an identification signal part indicating unlocking of the first digit in the head of the password signal for unlocking is received, in an extension telephone unlocking device 5, an extension telephone 12 for visitor reception is electrically disconnected from an extension telephone line 11 and the designation signal part and the password signal part of the identification signal part after the second digit are fetched. In the extension telephone unlocking device 1, it is judged whether a preset password **number** and the **password number** of the **password** signal part **match** or not. When the **password** numbers **match**, corresponding electronic locks 81 and 82 are unlocked for fixed time and a collated result matching signal is sent to the extension telephone sets 31-3n, to which the password signal for unlocking is inputted.

COPYRIGHT: (C)2003,JPO

27/5/1
JAPIO
(c) 2006 JPO & JAPIO. All rights reserved.
07473770 **Image available**

AUTHENTICATION DEVICE, AUTHENTICATION SYSTEM, AUTHENTICATION METHOD, AUTHENTICATION PROGRAM AND RECORDING MEDIUM

Pub. No.: 2002-342288 [JP 2002342288 A]
Published: November 29, 2002 (20021129)
Inventor: SAKURAZAWA TADASHI
Applicant: CASIO COMPUT CO LTD
Application No.: 2001-150361 [JP 2001150361]
Filed: May 21, 2001 (20010521)
International Class: G06F-015/00; G10L-015/00; G10L-015/28; H04L-009/32; H04Q-007/38

ABSTRACT

PROBLEM TO BE SOLVED: To provide an authentication device or the like capable of ensuring higher level security.

SOLUTION: A random number is generated (S201), and the combination of numerals and alphabets is decided, based on the generated random **number** (S202), and the **combination** of the numerals and alphabets is displayed (S204). A user recognizes the displayed contents, and inputs four alphabetical characters, corresponding to a **password** constituted own four digit numeral from a microphone. A control part fetches them (S205) and executes character recognition (S207). Whether or not all the characters, that is, those four characters can be recognized is discriminated (S208), and when it is determined that all the characters can be recognized, that is that the four alphabetical characters are converted into four-character numer based on the corresponding relation of the numerals and the alphabets (S209). Moreover, whether or not the converted four numerals are matched with the **password** of the user stored in a **password** storage part is discriminated (S210).

COPYRIGHT: (C)2003,JPO

27/5/5
JAPIO
(c) 2006 JPO & JAPIO. All rights reserved.
04942377 **Image available**

ROBBERY PREVENTING DEVICE FOR ELECTRONIC EQUIPMENT

Pub. No.: 07-234977 [JP 7234977 A]
Published: September 05, 1995 (19950905)
Inventor: KOIZUMI JUN
Applicant: HONDA MOTOR CO LTD [000532] (A Japanese Company or Corporation), JP (Japan)
Application No.: 06-051157 [JP 9451157]
Filed: February 23, 1994 (19940223)
International Class: [6] G08B-015/00; B60R-011/02; B60R-025/00
JAPIO Class: 44.9 (COMMUNICATION -- Other); 26.2 (TRANSPORTATION -- Motor Vehicles); 28.9 (SANITATION -- Other)

ABSTRACT

PURPOSE: To provide a robbery preventing device which can improve robbery the robbery preventing effect by increasing the **number of combinations** of **password** codes and without increasing the number of operating switches and also can eliminate a complicated input operation for electronic equipments.

CONSTITUTION: A robbery preventing device collates the **password** code inputted from an external input means with the codes stored in an internal memory and sets the usable/unusable state of an electronic equipment. Then the external input means of **password** codes consists of an item selector means which selects plural items and a numerical value setting means which sets the numerical value of each item in plural steps. In particular, these selector means end setting means serve as an acoustic control mode changeover switch 6 and a volume controller 3 or a bend changeover switch 5 which selects a receiving frequency band and a preset switch 4 which stores the receiving frequency respectively.

27/5/6
JAPIO
(c) 2006 JPO & JAPIO. All rights reserved.
02614766 **Image available**

PASSWORD COLLATING SYSTEM

Pub. No.: 63-231666 [JP 63231666 A]
Published: September 27, 1988 (19880927)
Inventor: SAITO TAKENORI
Applicant: NEC CORP [000423] (A Japanese Company or Corporation), JP (Japan)
Application No.: 62-065941 [JP 8765941]
Filed: March 20, 1987 (19870320)
International Class: [4] G06F-015/00; G06F-009/06
JAPIO Class: 45.4 (INFORMATION PROCESSING -- Computer Applications); 45.1 (INFORMATION PROCESSING -- Arithmetic Sequence Units)
Journal: Section: P, Section No. 818, Vol. 13, No. 35, Pg. 70, January 26, 1989 (19890126)

ABSTRACT

PURPOSE: To keep secret even if a **password** is leaked to the others, by collating the preliminarily registered **password** consisting of

plural digits and intervals of input time of respective digits as parameters to increase the **number** of **combinations** of the **password**.

CONSTITUTION: Intervals of input time of respective digits of the **password** consisting of plural digits inputted from a peripheral device 3 are counted by a time counter 3. Preliminarily determined intervals of input time of respective digits of the **password** consisting of plural prescribed digits are registered in a register file 5 with an allowable time width. A collating part 6 collates not only the **password** consisting of plural digits inputted from the peripheral device 3 but also intervals of input time of respective digits with preliminarily determined intervals of input time of respective digits. Since intervals of input time of the **password** are used as parameters, intervals of input time are on the outside of the input allowable range as the collation result and coincidence is not attained though the others obtains and uses the **password**, thus keeping the secret.

Keyword - NPL, bib

```
Set   Items  Description

S1     9950  S PASSWORD? ? OR PASSCODE? ? OR PASSPHRASE? ? OR PASS()(WORD? ? OR CODE? ? OR PHRASE? ?)

S2       28  S S1 (5N) (MATCH?? OR MATCHING)

S3      990  S S1 (5N) (BREAK??? OR BROKEN OR IDENTIFY OR IDENTIFIED OR DISCOVER?? OR (FOUND OR
FIND)()OUT OR DETERMINE? ? OR ASCERTAIN?? OR GUESS?? OR DEDUCE? ? OR (WORK OR FIGURE OR FIND)()OUT
OR DISCOVER?? OR DETERMINE? ? OR STOLEN OR STEAL OR EXTORT?? OR ATTACK?? )


S4      199  S S1 (3N) (GENERATED OR AUTOMAT? OR CANDIDATE? ? OR RANDOM)

S5        3  S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL) (3W) S4

S6        3  RD (unique items)

S7      115  S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL) (3W) S1

S8       14  S S7 (10N) ( PERIOD? OR DURATION? ? OR TIME OR S2 OR S3)

S9        8  S S8 NOT PY>2002

S10       6  RD  (unique items)

S11       6  S S10 NOT S6

S12    6576  S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL) (3W) (COMBINATION? ? OR
PERMUTATION? ? )

S13       1  S S12 AND S1

S14      75  S S1 (3N) (POSSIBLE OR POSSIBILITIES OR POTENTIAL OR MAXIMUM OR MAX OR FEASIBLE OR
FEASIBILITIES OR POSSIBILITIES )

S15       0  S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL)(3W) S14

S16       3  S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL)(3W) S4

S17      95  S S1 (3N) (PRODUCE? ? OR CONSTRUCT?? OR BUILT OR PREPARE? ? OR GENERATED)

S18       0  S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL)(3W) S17

; show files
```

[File 8] **Ei Compendex(R)** 1884-2006/Nov W1
(c) 2006 Elsevier Eng. Info. Inc. All rights reserved.
**File 8: The file has been reprocessed and accession numbers have changed. See HELP NEWS988 for details.*

[File 35] **Dissertation Abs Online** 1861-2006/Nov
(c) 2006 ProQuest Info&Learning. All rights reserved.

[File 65] **Inside Conferences** 1993-2006/Nov 27
(c) 2006 BLDSC all rts. reserv. All rights reserved.

[File 2] **INSPEC** 1898-2006/Nov W3
(c) 2006 Institution of Electrical Engineers. All rights reserved.

[File 94] **JICST-EPlus** 1985-2006/Aug W2
(c)2006 Japan Science and Tech Corp(JST). All rights reserved.

[File 111] **TGG Natl.Newspaper Index(SM)** 1979-2006/Nov 10
(c) 2006 The Gale Group. All rights reserved.

[File 6] **NTIS** 1964-2006/Nov W3
(c) 2006 NTIS, Intl Cpyrght All Rights Res. All rights reserved.

[File 144] **Pascal** 1973-2006/Nov W1
(c) 2006 INIST/CNRS. All rights reserved.

[File 434] **SciSearch(R) Cited Ref Sci** 1974-1989/Dec
(c) 2006 The Thomson Corp. All rights reserved.

[File 34] **SciSearch(R) Cited Ref Sci** 1990-2006/Nov W3
(c) 2006 The Thomson Corp. All rights reserved.

[File 62] **SPIN(R)** 1975-2006/Nov W2
(c) 2006 American Institute of Physics. All rights reserved.

[File 99] **Wilson Appl. Sci & Tech Abs** 1983-2006/Sep
(c) 2006 The HW Wilson Co. All rights reserved.

[File 95] **TEME-Technology & Management** 1989-2006/Nov W4
(c) 2006 FIZ TECHNIK. All rights reserved.

[File 56] **Computer and Information Systems Abstracts** 1966-2006/Nov
(c) 2006 CSA. All rights reserved.

[File 57] **Electronics & Communications Abstracts** 1966-2006/Nov
(c) 2006 CSA. All rights reserved.

[File 60] **ANTE: Abstracts in New Tech & Engineer** 1966-2006/Nov
(c) 2006 CSA. All rights reserved.

[File 266] **FEDRIP** 2006/Aug
Comp & dist by NTIS, Intl Copyright All Rights Res. All rights reserved.

[File 583] **Gale Group Globalbase(TM)** 1986-2002/Dec 13
(c) 2002 The Gale Group. All rights reserved.
**File 583: This file is no longer updating as of 12-13-2002.*

[File 438] **Library Lit. & Info. Science** 1984-2006/Sep
(c) 2006 The HW Wilson Co. All rights reserved.

[File 256] **TecInfoSource** 82-2006/May
(c) 2006 Info.Sources Inc. All rights reserved.

6/5/3 (Item 1 from file: 6)
Fulltext available through: Check for PDF Download Availability and Purchase

NTIS
(c) 2006 NTIS, Intl Cpyrght All Rights Res. All rights reserved.1413547 **NTIS Accession Number:** DE88016281
Framework for Password Selection

De Alvare', A. M. ; Schultz, E. E.
Lawrence Livermore National Lab., CA.
Corporate Source Codes: 068147000; 9513035
Sponsor: Department of Energy, Washington, DC.
Report Number: UCRL-99382; CONF-8808118-1
1988 15p
Language: English Document Type: Conference proceeding
Journal Announcement: GRAI8907; NSA1300
UNIX security workshop, Portland, OR, USA, 29 Aug 1988.
Portions of this document are illegible in microfiche products. Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)321-8547; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC A03/MF A01
Country of Publication: United States
Contract Number: W-7405-ENG-48
A major problem in computer security is intrusion into systems due to compromised authentication procedures. This paper focuses on the most commonly used authentication procedure--use of passwords. We have developed a framework for a methodology to estimate the guessability of passwords. We assume that passwords are usually based on a simple rule. If someone discovers one of a series of rule-based passwords, it is easier to guess other passwords. The framework we propose is that computer security experts can conduct guessability studies on a large **number** of **passwords** which are **candidates** for assignment to users. People who attempt to guess what a password is can be provided with cues, such as what a password for another account in the system is or a nickname. Hit rates (the percentage of passwords correctly guessed within a limited number of attempts) can then be obtained. This method can be used to develop metrics for guessability of classes of passwords. A system manager might utilize results of guessability studies by encouraging users to avoid choosing passwords which are closely associated with account names or which have been shown to be highly vulnerable to guessing, or by not assigning passwords which are from vulnerable classes of passwords. A pilot study confirmed the feasibility of this framework. Participants were given 20 attempts to guess an eight-character password which was either a common English word or two unrelated words joined by a control character (eight characters in all). The common English word was vulnerable to guessing, but only when cues about this word were provided. Participants never guessed the other password, however, even when cues were provided. The results not only demonstrate feasibility of our framework, but also suggest guidelines for selecting passwords which are less likely to result in compromised authentication procedures. 6 refs., 1 fig. (ERA citation 13:055993)
Descriptors: Computers; Computer Architecture; Safeguards; Security
Identifiers: *Computer security; *Computer privacy; ERDA/990220; NTISDE
Section Headings: 62GE (Computers, Control, and Information Theory--General)

11/5/1 (Item 1 from file: 8)
Fulltext available through: USPTO Full Text Retrieval Options SCIENCEDIRECT
Ei Compendex(R)
(c) 2006 Elsevier Eng. Info. Inc. All rights reserved.
07718208 **E.I. No:** EIP97063687733
Title: Number theoretic attacks on secure password schemes

Author: Patel, Sarvar
Corporate Source: Math and Cryptography Research Group, Morristown, NJ, USA
Conference Title: Proceedings of the 1997 IEEE Symposium on Security and Privacy
Conference Location: Oakland, CA, USA **Conference Date:** 19970504-19970507
Sponsor: IEEE
E.I. Conference No.: 46499
Source: Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy 1997. IEEE, Piscataway, NJ, USA,97CB36097. p 236-247
Publication Year: 1997

CODEN: PSSPEO **ISSN:** 1063-7109
Language: English
Document Type: CA; (Conference Article) **Treatment:** T; (Theoretical)
Journal Announcement: 9707W5
Abstract: Encrypted Key Exchange (EKE) allows two parties sharing a password to exchange authenticated information over an insecure network by using a combination of public and secret key cryptography. EKE promises security against active and dictionary attacks. Other secure protocols have been proposed based on the use of randomized confounders. We use some basic results from **number** theory to present **password** guessing **attacks** on all versions of EKE discussed in the paper and we also offer countermeasures to the attacks. However for the RSA version of EKE, we show that simple modifications are not enough to rescue the protocol. Attacks are also presented on half encrypted versions of EKE. We also show how randomized confounders cannot protect Direct Authentication Protocol and Secret Public Key Protocol versions of a secure password scheme from attacks. We discuss why these attacks are possible against seemingly secure protocols and what is necessary to make secure protocols. (Author abstract) 9 Refs.
Descriptors: *Security of data; Computer networks; Network protocols; Cryptography; Number theory; Random processes
Identifiers: Encrypted key exchange (EKE); Randomized confounders
Classification Codes:
723.2 (Data Processing); 922.1 (Probability Theory)
723 (Computer Software); 921 (Applied Mathematics); 922 (Statistical Methods)
72 (COMPUTERS & DATA PROCESSING); 92 (ENGINEERING MATHEMATICS)

11/5/3 (Item 1 from file: 2)
INSPEC
(c) 2006 Institution of Electrical Engineers. All rights reserved.
07314250 **INSPEC Abstract Number:** C1999-09-6130S-016
Title: A real-world analysis of Kerberos password security
Author Wu, T.
Author Affiliation: Dept. of Comput. Sci., Stanford Univ., CA, USA
Conference Title: Proceedings 1999 Network and Distributed System Security Symposium p. 13-22
Publisher: Internet Soc , Reston, VA, USA
Publication Date: 1999 **Country of Publication:** USA x+171 pp.
ISBN: 1 891562 04 5 **Material Identity Number:** XX-1999-00579
Conference Title: Proceedings of The Internet Society 1999 Network and Distributed System Security Symposium
Conference Sponsor: Internet Soc
Conference Date: 3-5 Feb. 1999 **Conference Location:** San Diego, CA, USA

Language: English **Document Type:** Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: Kerberos is a distributed authentication system that many organizations use to handle domain-wide password security. Although it has been known for quite some time that Kerberos is vulnerable to brute-force password searches, there has so far been little analysis of the scope and extent of this vulnerability. This paper discusses the nature of this weakness in detail and attempts to quantify the severity of the danger it poses to existing Kerberized installations. The results of a controlled experiment, in which a large **number** of **passwords** from a Kerberos realm were **broken** off-line and subjected to analysis, will be presented. The author explores possible strategies for repairing this security hole, the most viable of which is the use of Kerberos V5 preauthentication coupled with a secure password authentication protocol such as SRP, SPEKE, or EKE. (19 Refs)
Subfile: C
Descriptors: authorisation; cryptography; message authentication
Identifiers: Kerberos; distributed authentication system; domain-wide password security; brute-force password searches; vulnerability; security hole; Kerberos V5 preauthentication; secure password authentication protocol
Class Codes: C6130S (Data security); C1260C (Cryptography theory)
Copyright 1999, IEE

Keyword - NPL, fulltext

Set	Items	Description
S1	643261	S PASSWORD? ? OR PASSCODE? ? OR PASSPHRASE? ? OR PASS()(WORD? ? OR CODE? ? OR PHRASE? ?)
S2	854	S S1 (3N) (MATCH?? OR MATCHING)
S3	15437	S S1 (5N) (BREAK??? OR BROKEN OR IDENTIFY OR IDENTIFIED OR DISCOVER?? OR (FOUND OR FIND)()OUT OR DETERMINE? ? OR ASCERTAIN?? OR GUESS?? OR DEDUCE? ? OR (WORK OR FIGURE OR FIND)()OUT OR DISCOVER?? OR DETERMINE? ? OR STOLEN OR STEAL OR EXTORT?? OR ATTACK??)
S4	8494	S S1 (3N) (GENERATED OR AUTOMAT? OR CANDIDATE? ? OR RANDOM)
S5	275	S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL) (3W) S4
S6	3	S S5 (10N) (PERIOD? OR DURATION? ? OR TIME)
S7	7	S S5 (10N) (S2 OR S3)
S8	7	S S7 NOT S6
S9	7	S S8 NOT PY>2002
S10	3	RD (unique items)
S11	17840	S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL) (3W) (COMBINATION? ? OR PERMUTATION? ?)
S12	228	S S11 (30N) S1
S13	58	S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL) (3W) (S1 (3N) (PROPOSED OR POSSIBLE? ? OR POTENTIAL? ? OR VIABLE? ? OR POSSIBILITIES OR MAXIMUM OR MAX OR FEASIBLE OR FEASIBILITIES))
S14	31	S (NUMBER OR COUNT OR QUANTITY OR HOW()MANY OR TOTAL) (3W) (S1 (3N) (PRODUCE? ? OR CONSTRUCT?? OR BUILT OR PREPARE? ? OR GENERATED))
S15	0	S (RATIO OR RATIOS OR PERCENTAGE? ?) (10N) (S12 OR S13 OR S14)
S16	0	S (S12 OR S13) (30N) S14
S17	45396	S S1 (3N) (STRENGTH OR STRONG?? OR GOOD OR HIGH()QUALITY OR INTENSITY OR RESISTANCE OR VULNERABL? ? OR SECURE OR SECURITY)
S18	46	S (S12 OR S13) (30N) S17
S19	46	S S18 NOT S10
S20	13	S S19 NOT PY>2002
S21	9	RD (unique items)

; show files

[File 88] **Gale Group Business A.R.T.S.** 1976-2006/Nov 23
(c) 2006 The Gale Group. All rights reserved.

[File 369] **New Scientist** 1994-2006/Sep W3
(c) 2006 Reed Business Information Ltd. All rights reserved.

[File 160] **Gale Group PROMT(R)** 1972-1989
(c) 1999 The Gale Group. All rights reserved.

[File 635] **Business Dateline(R)** 1985-2006/Nov 28
(c) 2006 ProQuest Info&Learning. All rights reserved.

[File 15] **ABI/Inform(R)** 1971-2006/Nov 28
(c) 2006 ProQuest Info&Learning. All rights reserved.

[File 16] **Gale Group PROMT(R)** 1990-2006/Nov 27
(c) 2006 The Gale Group. All rights reserved.

[File 9] **Business & Industry(R)** Jul/1994-2006/Nov 27
(c) 2006 The Gale Group. All rights reserved.

[File 13] **BAMP** 2006/Nov W2
(c) 2006 The Gale Group. All rights reserved.

[File 810] **Business Wire** 1986-1999/Feb 28
(c) 1999 Business Wire . All rights reserved.

[File 610] **Business Wire** 1999-2006/Nov 28
(c) 2006 Business Wire. All rights reserved.
**File 610: File 610 now contains data from 3/99 forward. Archive data (1986-2/99) is available in File 810.*

[File 647] **CMP Computer Fulltext** 1988-2006/Jan W3
(c) 2006 CMP Media, LLC. All rights reserved.

[File 98] **General Sci Abs** 1984-2006/Oct
(c) 2006 The HW Wilson Co. All rights reserved.

[File 148] **Gale Group Trade & Industry DB** 1976-2006/Nov 24
(c)2006 The Gale Group. All rights reserved.

[File 634] **San Jose Mercury** Jun 1985-2006/Nov 23
(c) 2006 San Jose Mercury News. All rights reserved.

[File 275] **Gale Group Computer DB(TM)** 1983-2006/Nov 27
(c) 2006 The Gale Group. All rights reserved.

[File 47] **Gale Group Magazine DB(TM)** 1959-2006/Nov 24
(c) 2006 The Gale group. All rights reserved.

[File 75] **TGG Management Contents(R)** 86-2006/Nov W2
(c) 2006 The Gale Group. All rights reserved.

[File 636] **Gale Group Newsletter DB(TM)** 1987-2006/Nov 27
(c) 2006 The Gale Group. All rights reserved.

[File 624] **McGraw-Hill Publications** 1985-2006/Nov 28
(c) 2006 McGraw-Hill Co. Inc. All rights reserved.
**File 624: Homeland Security & Defense and 9 Platt energy journals added Please see HELP NEWS624 for more*

[File 484] **Periodical Abs Plustext** 1986-2006/Nov W3
(c) 2006 ProQuest. All rights reserved.

[File 613] **PR Newswire** 1999-2006/Nov 22
(c) 2006 PR Newswire Association Inc. All rights reserved.
**File 613: File 613 now contains data from 5/99 forward. Archive data (1987-4/99) is available in File 813.*

[File 813] **PR Newswire** 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc. All rights reserved.

[File 141] **Readers Guide** 1983-2006/Aug
(c) 2006 The HW Wilson Co. All rights reserved.

[File 239] **Mathsci** 1940-2006/Jan
(c) 2006 American Mathematical Society. All rights reserved.

[File 370] **Science** 1996-1999/Jul W3
(c) 1999 AAAS. All rights reserved.
**File 370: This file is closed (no updates). Use File 47 for more current information.*

[File 696] **DIALOG Telecom. Newsletters** 1995-2006/Nov 27
(c) 2006 Dialog. All rights reserved.

[File 553] **Wilson Bus. Abs.** 1982-2006/Oct
(c) 2006 The HW Wilson Co. All rights reserved.

[File 621] **Gale Group New Prod.Annou.(R)** 1985-2006/Nov 23
(c) 2006 The Gale Group. All rights reserved.

[File 674] **Computer News Fulltext** 1989-2006/Sep W1
(c) 2006 IDG Communications. All rights reserved.
**File 674: File 674 is closed (no longer updates).*

[File 20] **Dialog Global Reporter** 1997-2006/Nov 28
(c) 2006 Dialog. All rights reserved.

10/3,K/2 (Item 2 from file: 88)
Gale Group Business A.R.T.S.
(c) 2006 The Gale Group. All rights reserved.
03636346 **Supplier Number:** 16995253
Computer network insecurity: how to defend your confidential files.
Slavik, Donald H.; Peters, Thomas M.
Trial , 31 , n3 , 80(6)
March , 1995
ISSN: 0041-2538
Language: English **Record Type:** Fulltext; Abstract
Word Count: 3413 **Line Count:** 00265

...through a dictionary program to make sure that the password is not a valid English word.

Use long passwords. The number of characters in a **password determines how many random** combinations of characters a hacker (or hacking program) has to try in a brute-force attempt to guess it. The more characters used, the more...

21/3,K/2 (Item 2 from file: 15)
ABI/Inform(R)
(c) 2006 ProQuest Info&Learning. All rights reserved.
01830639 04-81630
Password security: An empirical study

Zviran, Moshe; Haga, William J
Journal of Management Information Systems: JMIS v15n4 pp: 161-185
Spring 1999
ISSN: 0742-1222 **Journal Code:** JMI
Word Count: 7659
Text:

...lists of words, including the standard online dictionary, name lists, and combinations of four-digit numbers (standing for the last four digits of a social **security number**), as **potential passwords**. It compared them against the actual passwords stored in the system file and gained access whenever a match was found.

Because the use of passwords...

21/3,K/4 (Item 2 from file: 16)
Gale Group PROMT(R)
(c) 2006 The Gale Group. All rights reserved.
01072380 **Supplier Number:** 41192182

Secrets
Miami Herald (FL) , p S19
Feb 26 , 1990
Language: English **Record Type:** Abstract
Document Type: Newspaper ; Trade

Abstract:

...are reprogrammable and range from -30,000 to 30,000 and the letters run from A to G. The first line of defense in computer **security**, the **password**, must be programmed first. Estevez says the **number** of possible personal **combinations** is 1.5 quadrillion.

21/3,K/7 (Item 1 from file: 275)
Gale Group Computer DB(TM)
(c) 2006 The Gale Group. All rights reserved.
01802864 **Supplier Number:** 17162300 **(Use Format 7 Or 9 For** FULL TEXT)
Making your customer's network secure.

Addelson, Roger
STACKS , v2 , n12 , p27(7)
Dec , 1994
ISSN: 1070-8596
Language: English **Record Type:** Fulltext; Abstract
Word Count: 4120 **Line Count:** 00341

...is sent to the system administrator. This may thwart an intruder who attempts a break4n using a computer to automatically generate and try a large **number** of ID/**password combinations**.

Even with this added security, a hacker who has access to the system may copy the **password**-authentication files and gain access to all **passwords**. Network and host **security** systems have become smarter and encrypted the password files, but this has not completely stopped criminals from breaking in. One creative hacker processed a computer...

21/3,K/8 (Item 1 from file: 624)
McGraw-Hill Publications

(c) 2006 McGraw-Hill Co. Inc. All rights reserved.

01282113

Goal for `Cyber Warrior' Training: Sharper Hacker Tactic Knowledge

By WILLIAM B. SCOTT

Aviation Week & Space Technology, Vol. 157,
No. 10, Pg 60
September 2, 2002
JOURNAL CODE: AW
SECTION HEADING: INFORMATION WARFARE ISSN: 0005-2175
WORD COUNT: 1,691

TEXT:

... to help federal agents track terrorist or other criminals' message traffic, but hackers use similar tools. Some can be remotely installed ``to get someone's **password** by watching network traffic," Bradley said.

-- **Password** crackers--automated tools that extract encrypted **passwords**. Some are ``brute-force" programs that try all letter and **number combinations** to get a match. The course teaches students what makes a **strong password** and will take considerable time to crack.

-- Rootkits--tools that alter security and system logs to hide a hacker's presence. ``They ensure a hacker...

STIC search for 10677277

Patent - fulltext

set	Items	Description
S1	41467	S PASSWORD? ? OR PASSCODE? ? OR PASSPHRASE? ? OR PASS()(WORD? ? OR CODE? ? OR PHRASE? ?)
S2	1601	S S1 (10N) (CHARACTER? ? OR LETTER? ?)
S3	1734	S S1 (5N) (PART OR PARTS OR PORTION? ? OR SECTION? ? OR SEGMENT? ? OR PIECE? ?)
S4	988	S S1 (10N) (PLACE OR PLACES OR POSITION? ?)
S5	14809	S (CHARACTER? ? OR LETTER? ?) (5N) (PLACE OR PLACES OR POSITION? ?)
S6	6	S S2 (5N) (RANK?? OR RANKING OR GRADE? ? OR GRADING OR SCORE? ? OR SCORING OR RATE? ? OR RATED OR RATING? ?)
S7	1043751	S TABLE? ? OR CHART? ?
S8	6	IDPAT S6 (sorted in duplicate/non-duplicate order)
S9	6	IDPAT S6 (primary/non-duplicate records only)
S10	19	S (S3 OR S4) (5N) (RANK?? OR RANKING OR GRADE? ? OR GRADING OR SCORE? ? OR SCORING OR RATE? ? OR RATED OR RATING? ?)
S11	19	S S10 NOT S9
S12	18	S S11 AND AY=1963:2002
S13	18	IDPAT (sorted in duplicate/non-duplicate order)
S14	18	IDPAT (primary/non-duplicate records only)
S15	294	S (S2 OR S3 OR S4) (5N) (STRENGTH OR STRONG?? OR GOOD OR HIGH()QUALITY OR INTENSITY OR RESISTANCE OR VULNERABL? ? OR SECURE OR SECURITY)
S16	144	S S2 (5N) (STRENGTH OR STRONG?? OR GOOD OR HIGH()QUALITY OR INTENSITY OR RESISTANCE OR VULNERABL? ? OR SECURE OR SECURITY)
S17	2	S S16 (30N) S7
S18	2	S S17 NOT (S9 OR S14)
S19	13	S S16 (30N) (MATCH?? OR MATCHING OR COMPARE? ? OR COMPARING OR COMPARISON? ? OR COMPARATOR? ? OR CONTRAST???)
S20	13	S S19 NOT (S9 OR S14 OR S18)
S21	8	S S20 AND AY=1963:2002
S22	8	IDPAT (sorted in duplicate/non-duplicate order)
S23	6	IDPAT (primary/non-duplicate records only)
S24	50	S S16 AND IC=H04L
S25	49	S S24 NOT (S9 OR S14 OR S18 OR S23)
S26	33	S S25 AND AY=1963:2002
S27	33	IDPAT (sorted in duplicate/non-duplicate order)

S28 18 IDPAT (primary/non-duplicate records only)

; show files

[File 348] **EUROPEAN PATENTS** 1978-2006/ 200648
(c) 2006 European Patent Office. All rights reserved.
**File 348: For important information about IPCR/8 and forthcoming changes to the IC= index, see HELP NEWSIPCR.*

[File 349] **PCT FULLTEXT** 1979-2006/UB=20061130UT=20061123
(c) 2006 WIPO/Thomson. All rights reserved.
**File 349: For important information about IPCR/8 and forthcoming changes to the IC= index, see HELP NEWSIPCR.*

[File 350] **Derwent WPIX** 1963-2006/UD=URL200677
(c) 2006 The Thomson Corporation. All rights reserved.
**File 350: DWPI has been enhanced to extend content and functionality of the database. For more info, visit http://www.dialog.com/dwpi/.*

9/5,K/1 (Item 1 from file: 350)
Derwent WPIX
(c) 2006 The Thomson Corporation. All rights reserved.

0014669636 *Drawing available*
WPI Acc no: 2005-017217/
XRPX Acc No: N2005-014632
Password authentication apparatus for mobile telephone, has CPU for prescribing useable function based on detection of grade of coincidence of password character code with reference password
Patent Assignee: FUJITSU TEN LTD (FUTE)
Inventor: ASHIDA T; IIZUKA K; YO S

Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
JP 2004341714	A	20041202	JP 2003135950	A	20030514	200502	B

Priority Applications (no., kind, date): JP 2003135950 A 20030514

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes
JP 2004341714	A	JA	19	8	

Alerting Abstract JP A
NOVELTY - A CPU (11) determines whether each character code of input password coincides with a reference password, and detects coincidence state that shows grade of coincidence. The CPU prescribes a useable function based on the detected coincidence state.
DESCRIPTION - An INDEPENDENT CLAIM is also included for password authentication method.
USE - For mobile telephone, navigation system, hands-free apparatus.
ADVANTAGE - Enables simplifying the operation, by accepting each function selectively and usably. Prevents releasing of security by other, easily.
DESCRIPTION OF DRAWINGS - The figure shows the structure of the password authentication apparatus used in hands-free system. (Drawing includes non-English language text).
1 hands-free system
10 memory
11 CPU

12 display

Title Terms /Index Terms/Additional Words: PASSWORD; AUTHENTICITY; APPARATUS; MOBILE; TELEPHONE; CPU; FUNCTION; BASED; DETECT; GRADE; COINCIDE; CHARACTER; CODE; REFERENCE

Class Codes

International Patent Classification

IPC	Class Level	Scope	Position	Status	Version Date
G06F-015/00			Main		"Version 7"
G06F-001/00			Secondary		"Version 7"

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-M06A1A; T01-N02B1B; W01-C01D3C; W01-C01Q8

Password authentication apparatus for mobile telephone, has CPU for prescribing useable function based on detection of grade of coincidence of password character code with reference password

14/5K/14 (Item 14 from file: 349)
PCT FULLTEXT
(c) 2006 WIPO/Thomson. All rights reserved.
01104876
METHOD AND SYSTEM FOR AUTHENTICATION
PROCEDE ET SYSTEME D'AUTHENTIFICATION

Patent Applicant/Inventor:

- **GELLER Avner**
  8 Motta Gur Street, 69694 Tel Aviv; IL; IL(Residence); IL(Nationality);
- **DARDIKMAN Shay**
  11 Fishman street, 64236 Tel-Aviv; IL; IL(Residence); IL(Nationality); (Designated only for: US)

Legal Representative:

- **REINHOLD COHN AND PARTNERS(agent)**
  P.O. Box 4060, 61040 Tel Aviv; IL;

	Country	Number	Kind	Date
Patent	WO	200428078	A1	20040401
Application	WO	2002IL781		20020923
Priorities	WO	2002IL781		20020923

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

[EP] AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES;
FI; FR; GB; GR; IE; IT; LU; MC; NL; PT;
SE; SK; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW;
ML; MR; NE; SN; TD; TG;

[AP] GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ;
UG; ZM; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Main International Patent Classes (Version 7):

IPC	**Level**
H04L-009/32	Main
G06F-001/00	
Publication Language:	English
Filing Language:	English
Fulltext word count:	13494

English Abstract:

Systems and methods for authentication of a user by an identification center are disclosed. A preferred embodiment of the invention includes the transfer over a communication medium of an encryption key to the user and/or the identification center, receipt by the identification center of a password encrypted by the user, simulation by the identification center of the encryption, comparison of the simulated encrypted password(s) with the received encrypted password, and authentication of the user if comparison results are sufficient. In another aspect of the invention, the encryption key is outputted by an identification center terminal and manually inputted into a user terminal.

French Abstract:

L'invention concerne des systemes et des procedes d'authentification d'un utilisateur par un centre d'identification. Un mode de realisation prefere de cette invention concerne le transfert par l'intermediaire d'un support de communication d'une cle de cryptage vers l'utilisateur et/ou le centre d'identification, la reception par le centre d'identification d'un mot de passe crypte par l'utilisateur, la simulation par le centre d'identification du cryptage, la comparaison du(des) mot(s) de passe crypte(s) simule(s) avec le mot de passe crypte recu et l'authentification de l'utilisateur dans le cas ou les resultats de la comparaison s'averent suffisants. Selon une autre variante, la cle de cryptage est fournie par un terminal de centre d'identification et entree manuellement dans un terminal utilisateur.

Type	Pub. Date	Kind	Text
Publication	20040401	A1	With international search report.

Detailed Description:

...necessarily the comparison results are sufficient to authenticate a user if one simulated encrypted password can be singled out as corresponding to the received encrypted **password**.

In one embodiment, as **part** of the comparison, a **score** is assigned to each simulated encrypted password and the simulated encrypted password with the best score, i.e. the closest match to the received encrypted...

23/5K/1 (Item 1 from file: 348)
EUROPEAN PATENTS
(c) 2006 European Patent Office. All rights reserved.
01753510
Authentication system and method based upon random partial pattern recognition
Authentifizierungs-System und -Verfahren basierend auf zufalliger partieller Mustererkennung
Systeme et procede d'authentification bases sur la reconnaissance de formes partielle aleatoire

Patent Assignee:

- **Authenture, Inc.**; (3934400)
  1958 Stratton Circle; Walnut Creek, California 94598; (US)
  (Applicant designated States: all)

Inventor:

- **Mizrah, Len L.**
  157 Glasgow Lane; San Carlos, CA 94070; (US)

Legal Representative:

- **Wright, Hugh Ronald (38053)**
  Brookes Batchellor, 102-108 Clerkenwell Road; London EC1M 5SA; (GB)

	Country	Number	Kind	Date	
Patent	EP	1434408	A2	20040630	(Basic)
	EP	1434408	A3	20041013	
Application	EP	2003258077		20031219	
Priorities	US	328640		20021223	

Designated States:
CH; DE; ES; FR; GB; IT; LI;

Extended Designated States:
AL; LT; LV; MK;

International Patent Class (V7): G06F-001/00; H04L-029/06**Abstract** EP 1434408 A2

An interactive client-server authentication system and method are based on Random Partial Pattern Recognition algorithm (RPPR). In RPPR, an ordered set of data fields is stored for a client (1010) to be authenticated in secure memory. An authentication server (1030) presents a clue to the client via a communication medium (1020), such positions in the ordered set of a random subset of data fields from the ordered set. The client enters input data in multiple fields according to the clue, and the server accepts the input data from the client via a data communication medium. The input data corresponds to the field contents for the data fields at the identified positions of the random subset of data fields. The server then determines whether the input data matches the field contents of corresponding data fields in a random subset.

Abstract Word Count: 139
NOTE: 1
NOTE: Figure number on first page: 1

Type	Pub. Date	Kind	Text
Application:	20040630	A2	Published application without search report
Change:	20041013	A2	International Patent Classification changed: 20040820
Search Report:	20041013	A3	Separate publication of the search report
Examination:	20050518	A2	Date of request for examination: 20050318
Assignee:	20050525	A2	Transfer of rights to new applicant: Authernative, Inc. (3934401) 1958 Stratton Circle Walnut Creek, California 94598 US
Examination:	20050622	A2	Date of dispatch of the first examination report: 20050509
Change:	20060628	A2	Title of invention (English) changed: 20060628
Change:	20060628	A2	Title of invention (French) changed: 20060628
Change:	20060823	A2	Title of invention (German) changed: 20060823
Change:	20060823	A2	Title of invention (English) changed: 20060823
Change:	20060823	A2	Title of invention (French) changed: 20060823

Publication: English

Procedural: English
Application: English

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200427	2104
SPEC A	(English)	200427	7209
Total Word Count (Document A) 9313			
Total Word Count (Document B) 0			
Total Word Count (All Documents) 9313			

Specification: ...WhiteFlower 12. Root: Z. Meter - field number before "Z" and behind "Z": oneZone, twoZtwo, threeZthree, ..., nineZnine.

These patterns are as easy to remember as 4 **character** PINs / **passwords**. However, the combinatorial **security** is a great deal of stronger for the RPPR based technology, as **compared** with SSPR algorithm based security systems.

Fig. 10 illustrates a client/server system including authentication resources according to the present invention. The client subsystem 1010...

23/5K/2 (Item 2 from file: 348)
EUROPEAN PATENTS
(c) 2006 European Patent Office. All rights reserved.
01258955
Operation of trusted state in computing platform
Betrieb von gesicherten Zustand in einer Computerplattform
Fonctionnement de l'etat securise sur une plate-forme d'ordinateur

Patent Assignee:

- **Hewlett-Packard Company**; (206030)
  3000 Hanover Street; Palo Alto, California 94304-1112; (US)
  (Applicant designated States: all)

Inventor:

- **Proudler, Graeme John**
  5 Touchstone Avenue; Meade Park, Bristol BS12 6XQ; (GB)

Legal Representative:

- **Lawman, Matthew John Mitchell et al (84552)**
  Hewlett-Packard Limited, IP Section, Building 3, Filton Road; Stoke Gifford, Bristol BS34 8QZ; (GB)

	Country	Number	Kind	Date	
Patent	EP	1085396	A1	20010321	(Basic)
Application	EP	99307380		19990917	

Designated States:
DE; FR; GB;

Extended Designated States:
AL; LT; LV; MK; RO; SI;

International Patent Class (V7): G06F-001/00**Abstract** EP 1085396 A1

A computing entity comprises a trusted monitoring component having a first processing means and a first memory means, the trusted monitoring component being a self-contained autonomous data processing unit, and a computer platform having a main processing

means and a main memory area, along with a plurality of associated physical and logical resources such as peripheral devices including printers, modems, application programs, operating systems and the like. The computer platform is capable of entering a plurality of different states of operation, each state of operation having a different level of security and trustworthiness. Selected ones of the states comprise trusted states in which a user can enter sensitive confidential information with a high degree of certainty that the computer platform has not been compromised by external influences such as viruses, hackers or hostile attacks. To enter a trusted state, references made automatically to the trusted component, and to exit a trusted state reference must be made to the trusted component. On exiting the trusted state, all references to the trusted state are deleted from the computer platform. On entering the trusted state, the state is entered in a reproducible and known manner, having a reproducible and known configuration which is confirmed by the trusted component.

Abstract Word Count: 206
NOTE: 7
NOTE: Figure number on first page: 7

Type	Pub. Date	Kind	Text
Application:	20010321	A1	Published application with search report
Assignee:	20010502	A1	Transfer of rights to new applicant: Hewlett-Packard Company, A Delaware Corporation (3016020) 3000 Hanover Street Palo Alto, CA 94304 US
Examination:	20010627	A1	Date of request for examination: 20010425
Change:	20060816	A1	Title of invention (German) changed: 20060816
Change:	20060816	A1	Title of invention (English) changed: 20060816
Change:	20060816	A1	Title of invention (French) changed: 20060816

Publication: English
Procedural: English
Application: English

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200112	1354
SPEC A	(English)	200112	11711
Total Word Count (Document A) 13065			
Total Word Count (Document B) 0			
Total Word Count (All Documents) 13065			

Specification: ...In order to make changes to the menu, various levels or security may be applied. For example, a user may be required to enter a **secure password**, for example a **password** comprising numbers and **letters** or other **characters** in step 1202. The trusted component monitors the trusted state from which the trusted component can be reconfigured by **comparing** measured integrity metrics from the computer platform whilst in the trusted state, with the set of pre-stored integrity metrics which the trusted component stores...

23/5K/5 (Item 5 from file: 349)
PCT FULLTEXT
(c) 2006 WIPO/Thomson. All rights reserved.
00837868

ELECTRONIC/MECHANICAL PASSWORD LOCKING/SECURITY SYSTEM EQUIPPED WITH INTERNAL HACKING PROTECTION PROGRAM USING TIME-INTERVAL
SYSTEME ELECTROMECANIQUE DE BLOCAGE ET SECURISATION D'UN MOT DE PASSE A PROGRAMME INTERNE DE HACHAGE A INTERVALLES DE TEMPS

Patent Applicant/Inventor:

- **MOON Gyu**
  Daewoo Apartment, 110-1303 Seoksa-Dong, Chunchon City, Kangwon-Do 200-180; KR; KR(Residence); KR(Nationality);

- **YUN Hyun**
  703-134 Mia 8-Dong, Gangbuk-Gu, Seoul 142-108; KR; KR(Residence); KR(Nationality);

Legal Representative:

- **CHO Chulhyun(agent)**
  Chun-il BLDG.5, 826-26 Yeoksam-Dong, Kangnam-Gu, Seoul 135-080; KR;

	Country	Number	Kind	Date
Patent	WO	200171497	A1	20010927
Application	WO	2001KR416		20010316
Priorities	KR	200013882		20000318

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

[EP] AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;
GR; IE; IT; LU; MC; NL; PT; SE; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GW; ML;
MR; NE; SN; TD; TG;

[AP] GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ;
UG; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Main International Patent Classes (Version 7):

IPC	**Level**
G06F-011/30	Main
Publication Language:	English
Filing Language:	Korean
Fulltext word count:	2491

English Abstract:

An electronic/mechanical password locking/security system equipped with internal hacking protection program using time-interval is disclosed. The electronic/mechanical password locking/security system comprises a custom semiconductor device (10) including a sequential comparator (14) for comparing an input password to a pre-stored password sequentially, a memory device (12) for storing an existing password and altering it, a timer (15) for outputting the existing password according to a predetermined time information, a clock/oscillator (16) for generating a basic time information of the system, an input buffer (13) for storing the input password and outputting the input password to the sequential comparator (14) according to a predetermined time information and a controller (11) for controlling and supervising the custom semiconductor device (10). According to the present invention, the system can maintain security using a time information between each character as well as a character information of input password even if a password is revealed, and maximize the security by adding a simple circuit to the conventional kinds of devices requiring security such as a mechanical locking device, a financial institution application, home, a military application and a satellite communication system.

French Abstract:

L'invention porte sur un systeme electromecanique de blocage et securisation d'un mot de passe a programme interne de hachage a intervalles de temps. Ledit systeme comporte: un dispositif semi-conducteur adapte (10) comportant un comparateur des sequences (14) du mot de passe introduit avec celles du mot de passe preenregistre; une memoire (12) stockant un mot de passe existant et le modifiant; un minuteur (15) emettant le mot de passe existant selon une information temporelle predetermine; une horloge (16) fournissant la base de temps du systeme; un tampon d'introduction (13) stockant le mot de passe introduit et le transmettant au comparateur (14) en fonction d'une information temporelle predeterminee; et un controleur (11) de commande et supervision du

dispositif semi-conducteur adapte (10). Ledit systeme assure la securite en utilisant une information temporelle entre chaque caractere ainsi qu'une information sur les caracteres du mot de passe introduit, meme s'il est revele, la securite etant encore accrue par l'adjonction d'un circuit simple a des dispositifs classiques devant etre securises tels que les dispositifs a blocage mecanique, les applications relatives a des etablissements financiers, les applications domestiques, les applications militaires, et les systemes de communication par satellite.

Type	Pub. Date	Kind	Text
Publication	20010927	A1	With international search report.
Examination	20020117		Request for preliminary examination prior to end of 19th month from priority date

Detailed Description:

...or counter.

Further, the present invention can be applied to a computer network system 2 0 hacking security device using a time information between each **character** of the input **password** when the user enters the **password**, a device for improving the **security** by sequentially **comparing** the

28/5K/9 (Item 9 from file: 348)
EUROPEAN PATENTS
(c) 2006 European Patent Office. All rights reserved.
01726048
Method to simplify the management and enhance the security of passwords
Verfahren zur vereinfachten Verwaltung und zur Steigerung der Sicherheit von Passworten
Procede pour faciliter le management et ameliorer la securite des mots de passe

Patent Assignee:

- **ABB RESEARCH LTD.**; (1524501)
  Affolternstrasse 52; 8050 Zurich; (CH)
  (Applicant designated States: all)

Inventor:

- **Dzung, Dacfey**
  Albisstrasse 1; 5430 Wettingen; (CH)

- **Bernasconi, Jakob**
  Fohrholzlistrasse 12 B; 5443 Niederrohrdorf; (CH)

Legal Representative:

- **ABB Patent Attorneys (101545)**
  c/o ABB Schweiz AG, Intellectual Property (CH-LC/IP), Brown Boveri Strasse 6; 5400 Baden; (CH)

	Country	Number	Kind	Date	
Patent	EP	1416666	A1	20040506	(Basic)
Application	EP	2002405914		20021028	

Designated States:
AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES;

FI; FR; GB; GR; IE; IT; LI; LU; MC; NL;
PT; SE; SK; TR;

Extended Designated States:
AL; LT; LV; MK; RO; SI;

International Patent Class (V7): H04L-009/32; H04L-009/32Abstract EP 1416666 A1

A method for simplifying the use and enhancing the storage security of non-fixed passwords is disclosed. It makes use of multiple passwords p1)), ..., pn)) and (n,m)-threshold schemes for storing the passwords on an access control medium and comprises: requesting the user to choose and enter n passwords p1)), ..., pn)) and computing n - m = s check values c1)),..., cs)) for m &lt; n from the n passwords p1)), ..., pn)) using a fixed (n x s)-matrix H; computing a one-way hash value c of the concatenation of p1)), ..., pn)) and storing the values c1)),..., cs)) and c; requesting the user at a subsequent login to enter m passwords pn1))))&hairsp;'),..., pnm))))&hairsp;') and computing the missing n-m = s passwords p1))&hairsp;') ,..., pn1))-1))&hairsp;') , pn1))+1))&hairsp;') ,..., pnm))-1))&hairsp;') ,pnm))+1))&hairsp;') ,...,pn))&hairsp;') from these passwords and the check values c1)),..., cs)); computing a hash value c' of the concatenation of p1))', ..., pn))', comparing the values c and c' and accepting the passwords if c = c'. Optionally, the method can provide for entering the m passwords at the subsequent login in any order. Furthermore, the values c1)),..., cs)) can be encrypted before storage and decrypted again before computing the missing n - m = s passwords p1))&hairsp;'),..., pn1))-1))&hairsp;'), pn1))+1))&hairsp;'),...,pnm))-1))&hairsp;'),pnm))+1))&hairsp;'),...,pn))&hairsp;'). Finally, a keyed one-way hash function F (message authentication code) can be used and the matrix H can be kept secret for additional protection.

Abstract Word Count: 234
NOTE: 1
NOTE: Figure number on first page: 1

Type	Pub. Date	Kind	Text
Application:	20040506	A1	Published application with search report
Withdrawal:	20050810	A1	Date application deemed withdrawn: 20041109

Publication: English
Procedural: English
Application: English

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200419	431
SPEC A	(English)	200419	2735
Total Word Count (Document A) 3166			
Total Word Count (Document B) 0			
Total Word Count (All Documents) 3166			

Specification: ...proposal regarding the first requirement, i.e., handling and organizing a plurality of different passwords for different applications, results in the following scheme: once a **"good" password** has been chosen, one or two of its **characters** are replaced by codes for the function of the **password** or by **letter**(s) of the name of the system the **password** is valid for - e.g., the chosen password Tbgw#D(vertical bar)3 is replaced by Tbg + (1st) letter of host) + #D(vertical bar) + (3rd... ...bar)3 -&gt; ... Finally, many proposals to meet the third requirement, i.e., creating a "hard" password, have been made. According to these proposals, a **good password** should include: lower and upper case **letters**, numbers, special **characters** like punctuation marks and mathematical symbols and extended ASCII characters. Proposed methods for generating a hard password include: using two unrelated words, pronounceable nonsense words...

28/5/1 (Item 1 from file: 350)
Derwent WPIX
(c) 2006 The Thomson Corporation. All rights reserved.

0013879537 *Drawing available*
WPI Acc no: 2004-058417/200406
XRPX Acc No: N2004-047181
Password entering method for e-banking system e.g. automatic teller machine, involves receiving codes corresponding to

characters entered by user while concealing entry on number of keys less than number of symbols
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: ANVEKAR D K

Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
US 6658574	B1	20031202	US 1999337720	A	19990621	200406	B

Priority Applications (no., kind, date): US 1999337720 A 19990621

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes
US 6658574	B1	EN	9	7	

Alerting Abstract US B1
NOVELTY - The method involves displaying distinct codes corresponding to characters in a users password. The codes entered serially by the user are received while an entry on a number of keys less than a number of symbols are concealed. The codes are entered as a number of key hits. The user enters each digit of a password by pressing a key a number of times corresponding to the digit. The digit entry is terminated by pressing another key.
USE - Used in e-banking system e.g. automatic teller machine (ATM).
ADVANTAGE - The method requires only few keys for concealing the keys, thereby preventing viewing of key entry during password entry. The method is very secure from password detection by casual observation of key hits during password entry. The method can coexist wit conventional password entry schemes as an option to be used when absolute security is required.
DESCRIPTION OF DRAWINGS - The drawing shows a pictorial view depicting concealment of keys to prevent videographing.

Title Terms /Index Terms/Additional Words: PASSWORD; ENTER; METHOD; BANK; SYSTEM; AUTOMATIC; TELLER; MACHINE; RECEIVE; CODE; CORRESPOND ; CHARACTER; USER; CONCEAL; NUMBER; KEY; LESS; SYMBOL

Class Codes

International Patent Classification

IPC	Class Level	Scope	Position	Status	Version Date
H04L-009/00			Main		"Version 7"
G06F-011/30; G06F-012/14; H04K-001/00; **H04L-009/32**			Secondary		"Version 7"

US Classification, Issued: 713202000, 713183000, 713184000, 380258000

File Segment: EPI;
DWPI Class: T01; T04; T05
Manual Codes (EPI/S-X): T01-N01A1; T01-N02B1B; T04-F01B; T05-L03C5

28/5/2 (Item 2 from file: 350)
Derwent WPIX
(c) 2006 The Thomson Corporation. All rights reserved.

0012619766 *Drawing available*
WPI Acc no: 2002-468270/
Related WPI Acc No: 2004-549400
XRPX Acc No: N2002-369395

Password authentication used on e.g. mobile telephone, involves pressing definition and direction keys to select character scroll on shown scroll areas and display characters recognized as password

Patent Assignee: CEC KK (CECC-N)
Inventor: KATO T; NAKAYAMA S

Patent Family (2 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
JP 2002140303	A	20020517	JP 2000334298	A	20001101	200250	B
JP 3546407	B2	20040728	JP 2000334298	A	20001101	200449	E

Priority Applications (no., kind, date): JP 2000334298 A 20001101

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
JP 2002140303	A	JA	7	7		
JP 3546407	B2	JA	9		Previously issued patent	JP 2002140303

Alerting Abstract JP A
NOVELTY - The method involves pressing definition keys (20) and a direction key (21) to select character scroll on the shown scroll areas (11-15) and display characters which are recognized as a password. The scroll areas show classified characters. The direction key can be used to transfer from one scroll area to another.
USE - Used in e.g. mobile telephone, personal digital assistant (PDA), personal handyphone system (PHS) terminal, portable personal computer.
ADVANTAGE - Ensures easy character input through simple key operation and correct confirmation of selected **characters** recognized as **password**. Maintains network **security** and simple operation without complicating network structure.
DESCRIPTION OF DRAWINGS - The figure shows the structure of the mobile telephone to which password authentication is applied. Drawing includes non-English language text.
11-15 Scroll areas
20 Definition keys
21 Direction key

Title Terms /Index Terms/Additional Words: PASSWORD; AUTHENTICITY; MOBILE; TELEPHONE; PRESS; DEFINE; DIRECTION; KEY; SELECT; CHARACTER; SCROLL; AREA; DISPLAY; RECOGNISE

Class Codes

International Patent Classification

IPC	Class Level	Scope	Position	Status	Version Date
G06F-015/00			Main		"Version 7"
G06F-003/00; **H04L-009/32**; H04M-001/727; H04Q-007/38			Secondary		"Version 7"

File Segment: EPI;
DWPI Class: T01; W01

Manual Codes (EPI/S-X): T01-C; T01-J; W01-A05B; W01-B05A; W01-C01D1D

28/5/3 (Item 3 from file: 350)
Derwent WPIX
(c) 2006 The Thomson Corporation. All rights reserved.

0009980125 *Drawing available*
WPI Acc no: 2000-282877/200024
XRPX Acc No: N2000-212918
Method of approving password in which each user has profile which specifies whether particular user's password should contain character from special subset of characters
Patent Assignee: HEIKKI O (HEIK-I); NOKIA NETWORKS OY (OYNO)
Inventor: HEIKKI O; OSMONEN H

Patent Family (5 patents, 86 countries)

Patent Number	**Kind**	**Date**	**Application Number**	**Kind**	**Date**	**Update**	**Type**
WO 2000011534	A1	20000302	WO 1999FI693	A	19990823	200024	B
FI 199801819	A	20000226	FI 19981819	A	19980825	200025	E
AU 199953757	A	20000314	AU 199953757	A	19990823	200031	E
FI 106281	B1	20001229	FI 19981819	A	19980825	200103	E
US 20010004759	A1	20010621	WO 1999FI693	A	19990823	200137	E
			US 2001777752	A	20010205		

Priority Applications (no., kind, date): FI 19981819 A 19980825

Patent Details

Patent Number	**Kind**	**Lan**	**Pgs**	**Draw**	**Filing Notes**	
WO 2000011534	A1	EN	16	2		
National Designated States,Original	AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW					
Regional Designated States,Original	AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW					
AU 199953757	A	EN			Based on OPI patent	WO 2000011534
FI 106281	B1	FI			Previously issued patent	FI 9801819
US 20010004759	A1	EN			Continuation of application	WO 1999FI693

Alerting Abstract WO A1
NOVELTY - Each user's profile includes an item specifying whether that particular user's **password** must contain one **character** selected from a set of special **characters**. This enables particularly important or **secure** users to have **passwords** including a wider range of **characters** and thus to be more difficult to break.
DESCRIPTION - An INDEPENDENT CLAIM is included for a system for approving a password.
USE - In data processing or information systems, in which used identifier is associated with a user profile.
ADVANTAGE - Provides additional security selectively for those users who require it.
DESCRIPTION OF DRAWINGS - The drawing illustrates a flowchart of operation of the embodiment of the invention.

Title Terms /Index Terms/Additional Words: METHOD; APPROVE; PASSWORD; USER; PROFILE; SPECIFIED; CONTAIN;

CHARACTER; SPECIAL; SUBSET

Class Codes

International Patent Classification

IPC	**Class Level**	**Scope**	**Position**	**Status**	**Version Date**
G06F-001/00; **H04L**; **H04L-009/32**			Main		"Version 7"
G06F; G06F-012/14			Secondary		"Version 7"

US Classification, Issued: 713202000, 713183000

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-H01C2; T01-J12C

28/5/5 (Item 5 from file: 350)
Derwent WPIX
(c) 2006 The Thomson Corporation. All rights reserved.

0009639605 *Drawing available*
WPI Acc no: 1999-591479/
XRPX Acc No: N1999-436326
Key generation from a given string to provide a password for network entity authentication
Patent Assignee: IBM CANADA LTD (IBMC)
Inventor: KOU W

Patent Family (2 patents, 1 countries)

Patent Number	**Kind**	**Date**	**Application Number**	**Kind**	**Date**	**Update**	**Type**
CA 2210763	A	19990117	CA 2210763	A	19970717	199951	B
CA 2210763	C	20000229	CA 2210763	A	19970717	200030	E

Priority Applications (no., kind, date): CA 2210763 A 19970717

Patent Details

Patent Number	**Kind**	**Lan**	**Pgs**	**Draw**	**Filing Notes**
CA 2210763	A	EN	24	7	
CA 2210763	C	EN			

Alerting Abstract CA A
NOVELTY - A process for generating an encryption key form a bit stream for a given character string comprises applying, at least repetitively, a combination of at least two bit stream processing operations. These are selected from a group of operations including bit stream splitting, recording and shuffling, bit-wise operations, and one-way hashing.
USE - For providing a scheme for generating a symmetric encryption key from a given string, such as a password, which can be used for network authentication.
ADVANTAGE - Passwords have no character limitation on the length or content of the given **character** string. This results in improved **security** and makes the **password** easier to remember for the user.

DESCRIPTION OF DRAWINGS - The drawing is a flow diagram illustrating a bit stream process used.

Title Terms /Index Terms/Additional Words: KEY; GENERATE; STRING ; PASSWORD; NETWORK; ENTITY; AUTHENTICITY

Class Codes

International Patent Classification

IPC	Class Level	Scope	Position	Status	Version Date
H04L-009/32			Main		"Version 7"

File Segment: EPI;
DWPI Class: W01
Manual Codes (EPI/S-X): W01-A05B

28/5/6 (Item 6 from file: 350)
Derwent WPIX
(c) 2006 The Thomson Corporation. All rights reserved.

0009148431 *Drawing available*
WPI Acc no: 1999-069981/
Related WPI Acc No: 1997-065056
XRPX Acc No: N1999-051275
Computer program for forming pronounceable security password used in encrypting and decrypting messages - is configured to generate pronounceable security password of eight characters or more including first word segment, if consecutive characters of first word segment is determined to be acceptable
Patent Assignee: BELL ATLANTIC NETWORK SERVICES (BELL-N)
Inventor: GANESAN R

Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
US 5850448	A	19981215	US 1994328226	A	19941025	199906	B
			US 1996731427	A	19961015		

Priority Applications (no., kind, date): US 1994328226 A 19941025; US 1996731427 A 19961015

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
US 5850448	A	EN	30	11	C-I-P of application	US 1994328226
					C-I-P of patent	US 5588056

Alerting Abstract US A
The computer program is configured to be readable from a computer readable storage medium and thereby causing a computer to operate so as to select a first one of the first and second word segment portions from the respective segment portions with equal probability. The selected first and second word segment portions are combined to form a first pronounceable word segment.
A judgement process then performed to check whether consecutive characters of the first pronounceable word segment are unacceptable due to their correspondence to those of first word segment portions having a transition number less than a first threshold

transition number. If the consecutive **characters** are determined to be acceptable, a pronounceable **security password** of eight or more **characters** including the first pronounceable word segment is generated.
ADVANTAGE - Generates user friendly pronounceable passwords which provide greater security.

Title Terms /Index Terms/Additional Words: COMPUTER; PROGRAM; FORMING; SECURE; PASSWORD; MESSAGE; CONFIGURATION; GENERATE; EIGHT; CHARACTER; MORE; FIRST; WORD; SEGMENT; CONSECUTIVE; DETERMINE; ACCEPT

Class Codes

International Patent Classification

IPC	**Class Level**	**Scope**	**Position**	**Status**	**Version Date**
H04L-009/00			Main		"Version 7"

US Classification, Issued: 380025000, 380004000, 380044000

File Segment: EPI;
DWPI Class: W01
Manual Codes (EPI/S-X): W01-A05B; W01-A06B5

NPL - bib

Set	Items	Description
S1	9995	S PASSWORD? ? OR PASSCODE? ? OR PASSPHRASE? ? OR PASS()(WORD? ? OR CODE? ? OR PHRASE? ?)
S2	776080	S CHARACTER? ? OR LETTER? ?
S3	127	S S1 (10N) S2
S4	83	S S1 (5N) (PART OR PARTS OR PORTION? ? OR SECTION? ? OR SEGMENT? ? OR PIECE? ?)
S5	57	S S1 (10N) (PLACE OR PLACES OR POSITION? ?)
S6	1	S S3 (5N) (RANK?? OR RANKING OR GRADE? ? OR GRADING OR SCORE? ? OR SCORING OR RATE? ? OR RATED OR RATING? ?)
S7	0	S (S4 OR S5) (5N) (RANK?? OR RANKING OR GRADE? ? OR GRADING OR SCORE? ? OR SCORING OR RATE? ? OR RATED OR RATING? ?)
S8	48	S (S3 OR S4 OR S5) (5N) (STRENGTH OR STRONG?? OR GOOD OR HIGH()QUALITY OR INTENSITY OR RESISTANCE OR VULNERABL? ? OR SECURE OR SECURITY)
S9	21	S S3 (5N) (STRENGTH OR STRONG?? OR GOOD OR HIGH()QUALITY OR INTENSITY OR RESISTANCE OR VULNERABL? ? OR SECURE OR SECURITY)
S10	8	S S9 NOT PY>2002
S11	5	RD (unique items)
S12	8685	S S2 (5N) (RANK?? OR RANKING OR GRADE? ? OR GRADING OR SCORE? ? OR SCORING OR RATE? ? OR RATED OR RATING? ?)
S13	10	S S12 AND S1
S14	10	S S13 NOT S11

```
S15     10  S S14 NOT PY>2002

S16     28  S S8 NOT PY>2002

S17     23  S S16 NOT (S11 OR S15)

S18     16  RD  (unique items)

; show files
```

[File 8] **Ei Compendex(R)** 1970-2006/Nov W4
(c) 2006 Elsevier Eng. Info. Inc. All rights reserved.
**File 8: The file has been reprocessed and accession numbers have changed. See HELP NEWS988 for details.*

[File 35] **Dissertation Abs Online** 1861-2006/Nov
(c) 2006 ProQuest Info&Learning. All rights reserved.

[File 65] **Inside Conferences** 1993-2006/Dec 06
(c) 2006 BLDSC all rts. reserv. All rights reserved.

[File 2] **INSPEC** 1898-2006/Nov W4
(c) 2006 Institution of Electrical Engineers. All rights reserved.

[File 94] **JICST-EPlus** 1985-2006/Aug W3
(c)2006 Japan Science and Tech Corp(JST). All rights reserved.

[File 111] **TGG Natl.Newspaper Index(SM)** 1979-2006/Nov 21
(c) 2006 The Gale Group. All rights reserved.

[File 6] **NTIS** 1964-2006/Nov W4
(c) 2006 NTIS, Intl Cpyrght All Rights Res. All rights reserved.

[File 144] **Pascal** 1973-2006/Nov W2
(c) 2006 INIST/CNRS. All rights reserved.

[File 434] **SciSearch(R) Cited Ref Sci** 1974-1989/Dec
(c) 2006 The Thomson Corp. All rights reserved.

[File 34] **SciSearch(R) Cited Ref Sci** 1990-2006/Dec W1
(c) 2006 The Thomson Corp. All rights reserved.

[File 62] **SPIN(R)** 1975-2006/Nov W4
(c) 2006 American Institute of Physics. All rights reserved.

[File 99] **Wilson Appl. Sci & Tech Abs** 1983-2006/Nov
(c) 2006 The HW Wilson Co. All rights reserved.

[File 95] **TEME-Technology & Management** 1989-2006/Dec W1
(c) 2006 FIZ TECHNIK. All rights reserved.

[File 56] **Computer and Information Systems Abstracts** 1966-2006/Nov
(c) 2006 CSA. All rights reserved.

[File 57] **Electronics & Communications Abstracts** 1966-2006/Nov
(c) 2006 CSA. All rights reserved.

[File 60] **ANTE: Abstracts in New Tech & Engineer** 1966-2006/Nov
(c) 2006 CSA. All rights reserved.

[File 266] **FEDRIP** 2006/Aug
Comp & dist by NTIS, Intl Copyright All Rights Res. All rights reserved.

[File 583] **Gale Group Globalbase(TM)** 1986-2002/Dec 13
(c) 2002 The Gale Group. All rights reserved.
**File 583: This file is no longer updating as of 12-13-2002.*

[File 438] **Library Lit. & Info. Science** 1984-2006/Nov
(c) 2006 The HW Wilson Co. All rights reserved.

[File 256] **TecInfoSource** 82-2006/Jun
(c) 2006 Info.Sources Inc. All rights reserved.

11/5/1 (Item 1 from file: 8)
Fulltext available through: USPTO Full Text Retrieval Options SCIENCEDIRECT
Ei Compendex(R)
(c) 2006 Elsevier Eng. Info. Inc. All rights reserved.
07695815 **E.I. No:** EIP97053657843
Title: Security of one-time signature

Author: Yen, Sung-Ming
Corporate Source: Da-Yeh Inst of Technology, Taiwan, China
Source: Electronics Letters v 33 n 8 Apr 10 1997. p 677-679
Publication Year: 1997
CODEN: ELLEAK **ISSN:** 0013-5194
Language: English
Document Type: JA; (Journal Article) **Treatment:** T; (Theoretical)
Journal Announcement: 9707W2
Abstract: Recently, Wu and Sung reported a one-time digital signature based on any one-way function in their article about password authentication. Owing to its general construction and potential applications, including the development of a one-time **password** scheme, in-depth **security** analysis is considered in the **Letter**. It is shown to suffer from a signature forgery problem. (Author abstract) 10 Refs.
Descriptors: *Security of data; Digital signal processing; Feature extraction
Identifiers: One time digital signature; One time password scheme; Password authentication
Classification Codes:
723.2 (Data Processing); 722.4 (Digital Computers & Systems); 723.5 (Computer Applications)
723 (Computer Software); 722 (Computer Hardware)
72 (COMPUTERS & DATA PROCESSING)

NPL - fulltext

Set	Items	Description
S1	645256	S PASSWORD? ? OR PASSCODE? ? OR PASSPHRASE? ? OR PASS()(WORD? ? OR CODE? ? OR PHRASE? ?)
S2	5614	S S1 (10N) (CHARACTER? ? OR LETTER? ?)
S3	4697	S S1 (5N) (PART OR PARTS OR PORTION? ? OR SECTION? ? OR SEGMENT? ? OR PIECE? ?)
S4	4706	S S1 (10N) (PLACE OR PLACES OR POSITION? ?)
S5	13	S S2 (5N) (RANK?? OR RANKING OR GRADE? ? OR GRADING OR SCORE? ? OR SCORING OR RATE? ? OR RATED OR RATING? ?)
S6	9	S S5 NOT PY>2002
S7	6	RD (unique items)

S8 18 S (S3 OR S4) (5N) (RANK?? OR RANKING OR GRADE? ? OR GRADING OR SCORE? ? OR SCORING OR RATE? ? OR RATED OR RATING? ?)

S9 18 S S8 NOT S7

S10 12 S S9 NOT PY>2002

S11 9 RD (unique items)

; show files

[File 88] **Gale Group Business A.R.T.S.** 1976-2006/Dec 04
(c) 2006 The Gale Group. All rights reserved.

[File 369] **New Scientist** 1994-2006/Sep W3
(c) 2006 Reed Business Information Ltd. All rights reserved.

[File 160] **Gale Group PROMT(R)** 1972-1989
(c) 1999 The Gale Group. All rights reserved.

[File 635] **Business Dateline(R)** 1985-2006/Dec 02
(c) 2006 ProQuest Info&Learning. All rights reserved.

[File 15] **ABI/Inform(R)** 1971-2006/Dec 07
(c) 2006 ProQuest Info&Learning. All rights reserved.

[File 16] **Gale Group PROMT(R)** 1990-2006/Dec 06
(c) 2006 The Gale Group. All rights reserved.

[File 9] **Business & Industry(R)** Jul/1994-2006/Dec 06
(c) 2006 The Gale Group. All rights reserved.

[File 13] **BAMP** 2006/Nov W3
(c) 2006 The Gale Group. All rights reserved.

[File 810] **Business Wire** 1986-1999/Feb 28
(c) 1999 Business Wire . All rights reserved.

[File 610] **Business Wire** 1999-2006/Dec 07
(c) 2006 Business Wire. All rights reserved.
**File 610: File 610 now contains data from 3/99 forward. Archive data (1986-2/99) is available in File 810.*

[File 647] **CMP Computer Fulltext** 1988-2006/Jan W4
(c) 2006 CMP Media, LLC. All rights reserved.

[File 98] **General Sci Abs** 1984-2006/Nov
(c) 2006 The HW Wilson Co. All rights reserved.

[File 148] **Gale Group Trade & Industry DB** 1976-2006/Dec 05
(c)2006 The Gale Group. All rights reserved.

[File 634] **San Jose Mercury** Jun 1985-2006/Dec 06
(c) 2006 San Jose Mercury News. All rights reserved.

[File 275] **Gale Group Computer DB(TM)** 1983-2006/Dec 06
(c) 2006 The Gale Group. All rights reserved.

[File 47] **Gale Group Magazine DB(TM)** 1959-2006/Dec 05
(c) 2006 The Gale group. All rights reserved.

[File 75] **TGG Management Contents(R)** 86-2006/Nov W3
(c) 2006 The Gale Group. All rights reserved.

[File 636] **Gale Group Newsletter DB(TM)** 1987-2006/Dec 06
(c) 2006 The Gale Group. All rights reserved.

[File 624] **McGraw-Hill Publications** 1985-2006/Dec 07
(c) 2006 McGraw-Hill Co. Inc. All rights reserved.
**File 624: Homeland Security & Defense and 9 Platt energy journals added Please see HELP NEWS624 for more*

[File 484] **Periodical Abs Plustext** 1986-2006/Dec W1
(c) 2006 ProQuest. All rights reserved.

[File 613] **PR Newswire** 1999-2006/Dec 07
(c) 2006 PR Newswire Association Inc. All rights reserved.
**File 613: File 613 now contains data from 5/99 forward. Archive data (1987-4/99) is available in File 813.*

[File 813] **PR Newswire** 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc. All rights reserved.

[File 141] **Readers Guide** 1983-2006/Oct
(c) 2006 The HW Wilson Co. All rights reserved.

[File 239] **Mathsci** 1940-2006/Jan
(c) 2006 American Mathematical Society. All rights reserved.

[File 370] **Science** 1996-1999/Jul W3
(c) 1999 AAAS. All rights reserved.
**File 370: This file is closed (no updates). Use File 47 for more current information.*

[File 696] **DIALOG Telecom. Newsletters** 1995-2006/Dec 07
(c) 2006 Dialog. All rights reserved.

[File 553] **Wilson Bus. Abs.** 1982-2006/Dec
(c) 2006 The HW Wilson Co. All rights reserved.

[File 621] **Gale Group New Prod.Annou.(R)** 1985-2006/Dec 04
(c) 2006 The Gale Group. All rights reserved.

[File 674] **Computer News Fulltext** 1989-2006/Sep W1
(c) 2006 IDG Communications. All rights reserved.
**File 674: File 674 is closed (no longer updates).*

[File 20] **Dialog Global Reporter** 1997-2006/Dec 07
(c) 2006 Dialog. All rights reserved.

7/3,K/1 (Item 1 from file: 16)
Gale Group PROMT(R)
(c) 2006 The Gale Group. All rights reserved.
05307074 **Supplier Number:** 48078952 **(USE FORMAT 7 FOR FULLTEXT)**

Unforgettable Biometrics
Phillips, Ken
PC Week , p 095
Oct 27 , 1997
Language: English **Record Type:** Fulltext
Document Type: Magazine/Journal; Tabloid ; General Trade
Word Count: 1606

...Web access-monitoring software, is nearing completion of its BioPassword software, which adds extra security to ordinary password systems.

BioPassword works by monitoring both the **rate** of typing and intervals between **letters**--the keystroke dynamics. Even if intruders guess the correct **password**, they probably cannot type it in with the proper rhythm unless they heard and memorized someone's key clicks.

BioPassword is scheduled for release sometime...